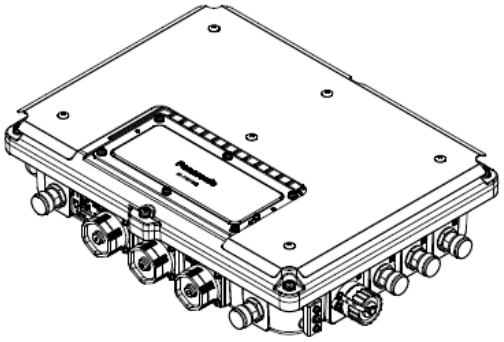
Panasonic

取扱説明書（設定編）

マルチアクセス コンセントレータ
920MHz 帯 通信ユニット

品番 EA-7TW11BS0

品番 EA-6HW11MS1



マルチアクセス コンセントレータ
EA-7TW11BS0

920MHz 帯 通信ユニット
EA-6HW11MS1

このたびは、パナソニック製品をお買い上げいただき、まことにありがとうございます。

- 取扱説明書（設定編）をよくお読みのうえ、正しく安全にお使いください。
- ご使用前に**「安全上のご注意」（10〜12 ページ）を必ずお読みください。**
- 保証書は「お買い上げ日・販売店名」などの記入を確かめ、製品に同梱の「安全上のご注意」とともに大切に保管してください。

はじめに

この取扱説明書(設定編)は、マルチアクセス コンセントレータ（EA-7TW11BS0）および 920MHz 帯 通信ユニット（EA-6HW11MS1）を利用される方が、正しく、安全に運用保守を行うことを目的として書かれています。各装置を取り扱う前にこの取扱説明書(設定編)をよく読み、書かれている指示や注意を十分に理解してください。また、この取扱説明書(設定編)は必要なときにすぐ参照できるよう使いやすい場所に保管してください。
マルチアクセス コンセントレータおよび 920MHz 帯 通信ユニットの設置については、各装置の「取扱説明書（工事編）」をお読みください。
＜商標について＞

- イーサネット/Ethernet は、富士ゼロックス株式会社の登録商標です。
- Microsoft とそのロゴ、Windows とそのロゴは米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- その他、本文中に記載の各会社名、各製品名は、各社の商標または、登録商標です。

＜ご使用にあたっての注意＞
パナソニック システムネットワークス株式会社は、本書に記述されている製品および技術に関する知的所有権を所有または管理しています。これらの製品、技術、および本書は、著作権法、特許権などの知的所有権に関する法律および国際条約により保護されています。

本書およびそれに付属する製品および技術は、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。パナソニック システムネットワークス株式会社およびそのライセンサーの書面による事前の許可なく、このような製品または技術および本書のいかなる部分も、いかなる方法によっても複製することが禁じられます。本書の提供は、明示的であるか黙示的であるかを問わず、マルチアクセス コンセントレータおよび 920MHz 帯 通信ユニットまたはそれに付随する技術に関するいかなる権利またはライセンスを付与するものでもありません。本書は、パナソニック システムネットワークス株式会社の一部、あるいはその関連会社のいかなる種類の義務を含むものでも示すものでもありません。

本書および本書に記述されている製品および技術には、ソフトウェアおよびフォント技術を含む第三者の知的財産が含まれている場合があります。これらの知的財産は、著作権法により保護されているか、または提供者からパナソニック システムネットワークス株式会社へライセンスが付与されているか、あるいはその両方です。

免責条項: 本書または本書に記述されている製品や技術に関してパナソニック システムネットワークス株式会社またはその関連会社が行う保証は、製品または技術の提供に適用されるライセンス契約で明示的に規定されている保障に限ります。このような契約で明示的に規定された保障を除き、パナソニック システムネットワークス株式会社およびその関連会社は、製品、技術、または本書に関して、明示、黙示を問わず、いかなる種類の保障も行いません。これらの製品、技術、または本書は、現状のまま提供され、商品性、特定目的への適合性または第三者の権利に対する非侵害の黙示の保障を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保障も、かかる免責が法的に無効とされた場合を除き、行われないものとします。

このような契約で明示的に規定されていない限り、パナソニック システムネットワークス株式会社またはその関連会社は、いかなる法理論のもとの第三者に対しても、その収益の損失、有用性またはデータに関する損失、あるいは業務の中断について、あるいは間接的損害、特別損害、付随的損害、または結果的損害について、そのような損害の可能性が示唆されていた場合であっても、適用される法律が許容する範囲内で、いかなる責任も負いません。

本書は、「現状のまま」提供され、商品性、特定目的への適合性または第三者の権利に対する非侵害の黙示の保障を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保障も、かかる免責が法的に無効とされた場合を除き、行われないものとします。

＜お知らせ＞

- Microsoft Corporation のガイドラインに従って画面写真を使用しています。
- この取扱説明書(設定編)の内容については、改良のため、予告なく変更する場合があります。
- この取扱説明書(設定編)の中で特にことわり書きがない場合は、「マルチアクセス コンセントレータ」、「コンセントレータ」は、マルチアクセス コンセントレータ（EA-7TW11BS0）のことを示しています。また、「通信ユニット」は、920MHz 帯 通信ユニット（EA-6HW11MS1）のことを示しています。

＜OSS（Open Source Software）ライセンス＞

コンセントレータのソフトウェアは、下記のオープンソースソフトウェアライセンスを使用しています。

“Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.”
“Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.”

（Open SSL License）

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

“Copyright・ 1998. Regents of the University of California All rights reserved.”

“THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

"Copyright (C) 2004, 2005 WIDE Project.All rights reserved. "

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

マルチアクセス コンセントレータについて

- コンセントレータの故障、誤動作、不具合、あるいは停電時の外部要因によって通話、録音等の機会を逸したために生じた損害等の純粋経済損害につきましては、当社は一切の責任を負いかねますので、あらかじめご了承ください。
- 地震、雷、風水害などの天災、火災、第三者による行為、その他の事故、お客様の故意、過失および誤用、その他異常な条件下での使用により生じた損害、およびコンセントレータの使用または使用不能から生ずる付随的な損害について、当社は一切の責任を負いかねますので、あらかじめご了承ください。
- コンセントレータは、医療機器、生命維持装置、航空交通管制機器、その他人命に関わる機器・装置・システムでの使用を意図しておりません。コンセントレータをこれらの機器・装置・システムなどに使用され生じた損害について、当社は責任を負いかねますので、あらかじめご了承ください。

920MHz 帯 通信ユニットについて

- 通信ユニットの故障、誤動作、不具合、或いは停電時の外部要因によって生じた損害等の純粋経済損害につきましては、当社は一切の責任を負いかねますので、あらかじめご了承ください。
- 地震、雷、風水害などの天災、火災、第三者による行為、その他の事故、お客様の故意、過失および誤用、取り付け不備、その他異常な条件下での使用により生じた損害、および通信ユニットの使用または使用不能から生ずる付随的な損害について、当社は一切の責任を負いかねますので、あらかじめご了承ください。
- 通信ユニットは、医療機器、生命維持装置、航空交通管制機器、その他人命に関わる機器・装置・システムでの使用を意図しておりません。通信ユニットをこれらの機器・装置・システムなどに使用され生じた損害について、当社は責任を負いかねますので、あらかじめご了承ください。

もくじ

はじめに 2

安全上のご注意 10

使用上のお願い 13

電波に関する留意点 15

無線 LAN 製品ご使用時におけるセキュリティに関するご注意 17

第 1 章　概要 18

1.1　製品構成 19

1.2　製品の特長 20

1.3　各部位の説明 30

第 2 章　設定の準備 36

2.1　Web コンソール用パソコンの設定 37

2.2　Web でのログイン・ログアウト 41

2.3　ユーザ名・パスワードの変更 43

2.4　CLI コンソールでのログイン・ログアウト 45

第 3 章　装置の基本設定 50

3.1　基本設定の流れ 51

3.2　IP インターフェースの設定 55

3.3　SSID の設定 57

3.4　SSID 多重設定 64

3.5　SSID 設定情報コピー 67

3.6　各無線インターフェースの設定 68

第 4 章　各種機能設定 74

4.1　QoS 75

4.1.1 SSID ごとの帯域制限 75
4.1.2 フローごとの優先制御 79
4.2 セキュリティ設定 83
4.2.1 認証と暗号化 83
4.2.2 認証方式と暗号化方式の組み合わせ 85
4.2.3 Authentication サーバを利用した IEEE802.1X 認証 92
4.2.4 ユーザ認証 100
4.3 自動干渉回避 104
4.3.1 無線監視設定 104
4.3.2 送受信チャネル自動変更 105
4.3.3 隣接 AP・干渉 AP の確認 108
4.3.4 レーダー監視 113
4.3.5 周波数帯域幅復旧 114
4.4 フィルタリング 116
4.5 無線ブリッジ 128
4.6 VoIP 利用時の各種設定 134
4.6.1 通話数制限機能 134
4.6.2 代理 ARP 応答 142
4.6.3 VoIP/Video 自動優先割り当て 144
4.7 サービス品質向上機能 145
4.7.1 5GHz 帯への端末誘導設定 145
4.7.2 小セル化（ビーコンレートの指定） 147
4.7.3 同時接続端末数制御 149
4.7.4 最低接続保障台数制御 152
4.7.5 IGMP スヌーピング 155

4.7.6 Passpoint 機能 159
4.8 Web 認証 171
4.8.1 Web 認証一覧 171
4.8.2 Web 認証 AP 間連携 180
4.9 PoE 給電 182
4.9.1 PoE 給電有効無効設定 182
4.9.2 PoE 給電状態の確認 185
4.10 その他の機能 191
第 5 章 VPN ネットワーク対応 196
5.1 L2TP over PPPoE ネットワーク接続での設定 197
5.2 L2TP over IPsec ネットワーク接続での設定 207
第 6 章 920MHz 帯 ネットワーク 214
6.1 920MHz 帯ネットワーク概要 215
6.1.1 特長 215
6.1.2 構成例 215
6.2 ネットワーク設定 217
6.2.1 IP アドレス設定 217
6.2.2 SNMP 設定 220
6.2.3 TRAP 通知設定 222
6.2.4 センサデータ制御元設定 224
6.2.5 センサデータ制通知先設定 226
6.3 920MHz 帯ネットワーク設定 228
6.3.1 サービス ID 設定 228
6.3.2 端末登録 231
6.3.3 920MHz 帯無線設定 233

第７章　保守 235
7.1　設定データのバックアップと読み込み 236
7.1.1　設定データのバックアップ 236
7.1.2　設定データの読み込み 240
7.1.3　全設定一括バックアップ 243
7.1.4　全設定一括読み込み 247
7.2　ファームウェアのアップデート 250
7.3　ログ機能 255
7.3.1　ログ一覧 255
7.3.2　記録・表示 257
7.3.3　TFTP によるリモート採取 263
7.3.4　ログの初期化 266
7.3.5　干渉情報ログ・パケットログ・統計情報ログの読出し 268
7.4　遠隔無線通信状態の確認 269
7.5　時刻設定 271
7.6　装置の初期化 274
保証とアフターサービス(よくお読みください) 278

なお関連の機器の取扱説明書（本取扱説明書とは別冊）を合わせてお読みください。
各取扱説明書には以下の内容の記載があります。

マルチアクセス コンセントレータ「取扱説明書（工事編）」
＜置局設計編＞　仕様、置局設計
＜施工編＞　　装置仕様、設置工事、オプション製品の設置、推奨品、障害発生時の対処方法

920MHz 帯 通信ユニット「取扱説明書（工事編）」
＜置局設計編＞　仕様、置局設計
＜施工編＞　　装置仕様、設置工事、推奨品、障害発生時の対処方法

安全上のご注意　必ずお守りください

安全上のご注意

人への危害、財産の損害を防止するため、必ずお守りいただくことを説明しています。

■誤った使い方をしたときに生じる危害や損害の程度を区分して、説明しています。

⚠ 警告	「死亡や重傷を負うおそれがある内容」です。
⚠ 注意	「軽傷を負うことや、財産の損害が発生するおそれがある内容」です。

■お守りいただく内容を次の図記号で説明しています。（次は図記号の例です）

	してはいけない内容です。
	実行しなければならない内容です。

安全上のご注意　必ずお守りください

⚠警告

 ぬれ手禁止	**■ぬれた手で配線工事をしない** 感電の原因になります。
 分解禁止	**■分解・改造をしない** 火災・感電の原因になります。
 禁止	**■ブレーカや配線器具の定格を超える使い方や、指定以外の電圧での使用はしない** 定格を超えると、発熱による火災の原因になります。
	■自動ドア、火災報知器などの自動制御機器の近くには設置しない コンセントレータからの電波が自動制御機器に影響を及ぼすことがあり、誤動作による事故の原因になります。
	■医療機器の近くには設置しない コンセントレータからの電波が、医療機器に影響を及ぼすことがあり、誤動作による事故の原因になります。
	■電源コード・電源コネクタ本体を破損するようなことはしない （傷つける、加工する、熱器具に近づける、無理に曲げる、ねじる、引っ張る、重い物を載せる、束ねる　など） 感電・ショート・火災の原因になります。
	■920MHz 帯 通信ユニットを水につけたり、水をかけたり、ぬらしたりしない ショートにより、火災や感電の原因になります。
	■腐食性ガスの発生する場所に設置しない 取り付け部が劣化して、落下など事故の原因になります。
	■荷重に耐えられない場所や不安定な場所には設置しない 落下など事故の原因になります。
	■雷が発生したときは、コンセントレータ・通信ユニットや電源コネクタ・電源コード・接続したケーブル類・アンテナ・バンドパスフィルター・固定用の取付金具類に触れない 感電の原因になります。
	■電源を入れたまま配線工事をしない 感電の原因になります。

安全上のご注意　必ずお守りください

⚠ 警告

禁止	**■使用を終了した装置は、放置しない** そのまま放置しておくと、落下など事故の原因になります。
必ず守る	**■心臓ペースメーカーの装着部位から 22cm 以上離す** 電波によりペースメーカーの作動に影響を与える場合があります。
	■煙が出たり、異常発熱したり、異臭・異音がした場合や落下・破損した場合は、電源コネクタを本体から抜き、コンセントレータ・通信ユニットの使用を中止する そのまま使用すると火災や感電の原因になります。 ●すぐに使用を中止し、修理依頼窓口にご相談ください。
	■モルタル壁などへの取り付け時、取付金具、ねじ等をメタルラス、ワイヤラスまたは金属板と接触しないように設置する 装置の絶縁が劣化した場合、メタルラス等に漏電し、火災の原因になります。
アース線接続	**■アースを確実に取り付ける** 感電や機器の動作が不安定になる原因になります。

⚠ 注意

禁止	**■工事中にコンセントレータ・通信ユニットを落下させない** けがの原因になることがあります。
	■高温になる場所に設置しない 装置内部の温度が上がり、火災や感電の原因になることがあります。
	■金属のエッジを手でこすらない 強くこすると、けがの原因になることがあります。
必ず守る	**■長時間使用しないときや、お手入れ、保守をするときは必ず電源プラグをコンセントから抜く** 漏電・感電の原因になることがあります。
	■取り付け設置時、指定の固定方法で取り付けをする 正しく設置を行わないと、ゆるみやはずれで落下し、事故の原因になることがあります。 ●設置方法については、必ず取扱説明書(工事編)をお読みください。

使用上のお願い

- **設置工事業者以外は取り付け工事を行わないでください。**
  正しく設置を行わないと、ゆるみやはずれで落下し、事故の原因になります。

- **ラジオ・テレビ・無線機などの磁気、電磁波を発生するものの近くに設置しないでください。また、そのようなものを近づけないでください。**
  ラジオやテレビに雑音が入ることがあります。また、コンセントレータ・通信ユニットが正常に動作しないことがあります。

- **受信用テレビアンテナからなるべく距離を離して設置してください。**
  テレビに受信障害などの影響を与えることがあります。テレビ電波の弱い地域ではなるべく距離を離して設置してください。

- **インターフェースケーブルの接続や初期設定時の PC 接続等で使用装置内部の操作を行う際は、帯電しにくい衣服および靴（静電気対策品）を着用してください。**
  静電気により、障害発生や装置故障の原因となります。

- **停電や電源瞬断に対して、バッテリー等の保護手段を用意しておりません。**
  システムを安定的に稼動させる必要がある場合には、無停電電源装置などのご使用をおすすめします。

- **暖房設備、ボイラーなどの、特に温度の上がる場所に置かないでください。**
  機器表面や部品が変形・劣化するほか、故障の原因になります。

- **火気を近づけないでください。**
  機器表面や部品が変形・劣化するほか、故障の原因になります。

- **硫化水素、リン、アンモニア、硫黄、炭素、酸、塵埃、その他有毒ガスなどの発生する場所に置かないでください。**
  故障や機器の寿命が短くなる原因になります。

- **電磁波発生源や磁気を帯びたもののある場所に置かないでください。（高周波ミシン・電気溶接機・磁石など）**
  雑音の発生や故障の原因になります。

- **機器に強い衝撃や振動を与えないでください。**
  落としたりぶつけたりして強い衝撃が加わると、故障や破損の原因になります。

- **経年変化により変色することがあります。**
  太陽光や雨などの影響で若干コンセントレータ・通信ユニットの色は変化しますが、性能には影響ありません。

- **雨の後などに作業を行う場合、装置についた雨水を十分にふき取った後に作業してください。**
  カバーを開く際内部に水が浸入し、故障の原因になります。

- **お手入れをするときは、電源を切った状態で行ってください。機器は、乾いた柔らかい布でふいてください。**
  汚れがひどい場合は、柔らかい布に薄めた台所用洗剤（中性）をしみこませ、固く絞ったものでふき、乾いた柔らかい布で仕上げてください。
  アルコール、石油、シンナー、ベンジン、熱湯、みがき粉、粉せっけん、ワックスなどは使わないでください。殺虫剤などの揮発性のものをかけたりしないでください。また、ゴムやビニール、粘着テープなどを長時間接触させないでください。変形、変色の原因となることがあります。
  化学ぞうきんをご使用の場合は、その注意書に従ってください。

- **廃棄時は、産業廃棄物として適切に処理してください。**

- **譲渡・廃棄時は、工場出荷時初期化機能を用いて、初期化してください。**
  ID/パスワードや、ネットワーク設定などの情報が漏えいする原因になります。

電波に関する留意点

- マルチアクセス コンセントレータ、および、920MHz 帯 通信ユニットは、電波法に基づく無線設備（920MHz 帯特定小電力通信システム、2.4GHz 帯高度化小電力データ通信システムおよび 5GHz 帯小電力データ通信システム、5GHz 帯無線アクセスシステム）の技術基準への適合が証明されています。5GHz 帯無線アクセスシステムを使用するときのみ、無線局の免許が必要となります。また、日本国内のみで使用できます。

- マルチアクセス コンセントレータおよび 920MHz 帯 通信ユニットは、技術基準の適合が証明されておりますので、以下の事項を行うと法律により罰せられることがあります。
  ■装置を分解／改造すること（周波数帯、アンテナの変更をしてはいけない）
  ■装置に貼ってある認証ラベルをはがすこと

- 5GHz 帯（IEEE802.11a/n）は電波法により屋外で使用可能な周波数が制限されています。
  ■5GHz 帯（IEEE802.11a/n）の対応チャネルは、100ch ～ 140ch（W56）です。
  ■W56 に対応するため、電波制御機能 DFS、TPC が使用されています。

- 4.9GHz 帯（IEEE802.11j）では、コンセントレータに接続するアンテナに従って、BPF（バンドパスフィルター）の接続が必要です。誤った組み合わせや BPF を未接続のままで使用すると、電波法違反になりますので、正しい組み合わせでご使用ください。
  ■4.9GHz 帯（IEEE802.11j）の対応チャネルは、184ch～196ch です。

- 2.4 GHz 帯（IEEE802.11b/g/n）の使用周波数帯では、電子レンジや産業・科学・医療機器のほか工場の製造ラインなどで使用されている移動体識別用の構内無線局（免許を要する無線局）および特定小電力無線局（免許を要しない無線局）が運用されています。
  ■コンセントレータを使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局、
  およびアマチュア無線局が運用されていないことを確認してください。
  ■万一、コンセントレータから移動体識別用の構内無線局に対して有害な電波干渉の事例が
  発生した場合には、すみやかにコンセントレータの使用周波数を変更して、
  電波干渉をしないようにしてください。
  ■その他、コンセントレータから移動体識別用の特定小電力無線局あるいはアマチュア無線局に対して
  有害な電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、
  ご購入になった販売窓口までご連絡ください。
  使用周波数帯域 ：2.4GHz
  変調方式 ：DS-SS 方式／ OFDM 方式
  想定干渉距離 ：40 m 以下
  周波数変更の可否 ：全帯域を使用し、かつ「構内無線局」「特定小電力無線局」帯域を回避可能
  コンセントレータには、これを示す右記のマークが貼付されます。

- コンセントレータ、および、通信ユニットは、電波法に基づく無線設備（920MHz 帯特定小電力通信システム）の技術基準への適合が証明されています。従って、当該装置を使用するときに無線局の免許は必要ありません。また、日本国内のみで使用できます。

- コンセントレータ、および、通信ユニットは、技術基準への適合が証明されておりますので、以下の事項を行うと法律により罰せられることがあります。
  - 装置、およびアンテナを分解／改造すること（周波数、アンテナの変更をしてはいけない）
  - 装置の内部に貼ってある認証ラベルをはがすこと
  - 規定以外のアンテナおよび給電線を使用すること

- 920MHz 帯は特定小電力無線局（免許を要しない無線局）が運用されています。
  - ■ 装置を使用する前に、近くで特定小電力無線局が運用されていないことを確認してください。
  - ■ 万一、装置から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、すみやかに装置の使用周波数を変更して、電波干渉をしないようにしてください。

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

- 無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコンなどとコンセントレータ間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。

  その反面、電波はある範囲内であれば障害物（壁など）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

  ■ 通信内容を盗み見られる
  ・悪意ある第三者が、電波を故意に傍受し、
  ID やパスワードまたはクレジットカード番号などの個人情報
  メールの内容
  などの通信内容を盗み見られる可能性があります。

  ■ 不正に侵入される
  ・悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、
  個人情報や機密情報を取り出す（情報漏えい）
  特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
  傍受した通信内容を書き換えて発信する（改ざん）
  コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）
  などの行為をされてしまう可能性があります。

本来、無線 LAN カードやマルチアクセス コンセントレータは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

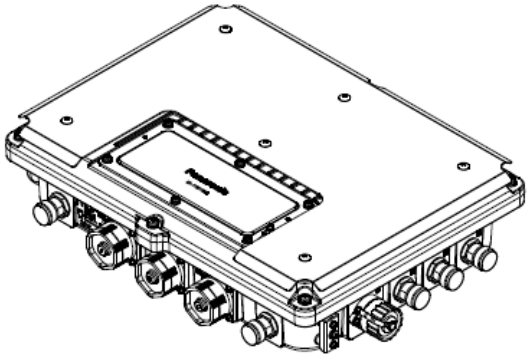
セキュリティの設定を行わないで使用した場合の問題を十分理解したうえで、お客様自身の判断と責任においてセキュリティに関する設定を行い、あわせてご使用になられる環境に応じたその他対応（物理的なセキュリティによる盗難対策や VPN 機能の利用による盗聴防止など）を行ったうえで製品を使用することをおすすめします。
特にマルチアクセス コンセントレータと 920MHz 帯 通信ユニット間の 920MHz 帯での通信においては、セキュリティの仕組みは持っておりません。ご注意ください。

第１章　概要

製品構成および特長を紹介します。

1.1　製品構成

マルチアクセス コンセントレータ本体、920MHz 帯 通信ユニット、オプション品、推奨品（PoE インジェクタ、アンテナ等）で構成されます。オプション品、推奨品は、マルチアクセス コンセントレータ「取扱説明書（工事編）」、920MHz 帯 通信ユニット「取扱説明書（工事編）」を参照ください。



マルチアクセス コンセントレータ
EA-7TW11BS0

920MHz 帯 通信ユニット
EA-6HW11MS1

1.2　製品の特長

コンセントレータは、（1）5GHz 無線（4.9GHz 帯）を用いた長距離中継通信機能、（2）公衆／プライベートサービス共存が可能な Wi-Fi 対応端末を収容する 2.4G/5GHz デュアルバンド Wi-Fi 基地局機能、（3）920MHz 特定小電力通信システムによって通信ユニットに接続された様々なセンサ機器からの情報等を収集する機能までを 1 台で実現します。
従来は、個々の通信機器を手配し、お互いの干渉を考慮して設置しなければなりませんでしたが、コンセントレータは相互干渉を抑制して 1 つの筐体内に収容し、オールインワン化を実現しました。なお、コンセントレータは、幅 350mm×高さ 76mm×奥行き 260mm のコンパクト設計で、防塵防水規格の IP66 仕様となっています。

1.2.1.　5GHz 無線（4.9GHz 帯）を用いた長距離中継通信の実現

コンセントレータでは、高出力可能な 4.9GHz 帯により見通しで最長 50km 通信、近距離では最大 450Mbps で通信が可能です。また、ダイバーシチ機能により海上伝搬にも対応できるほか、2 ポート装備により中継地点も 1 台で多段接続が可能です。

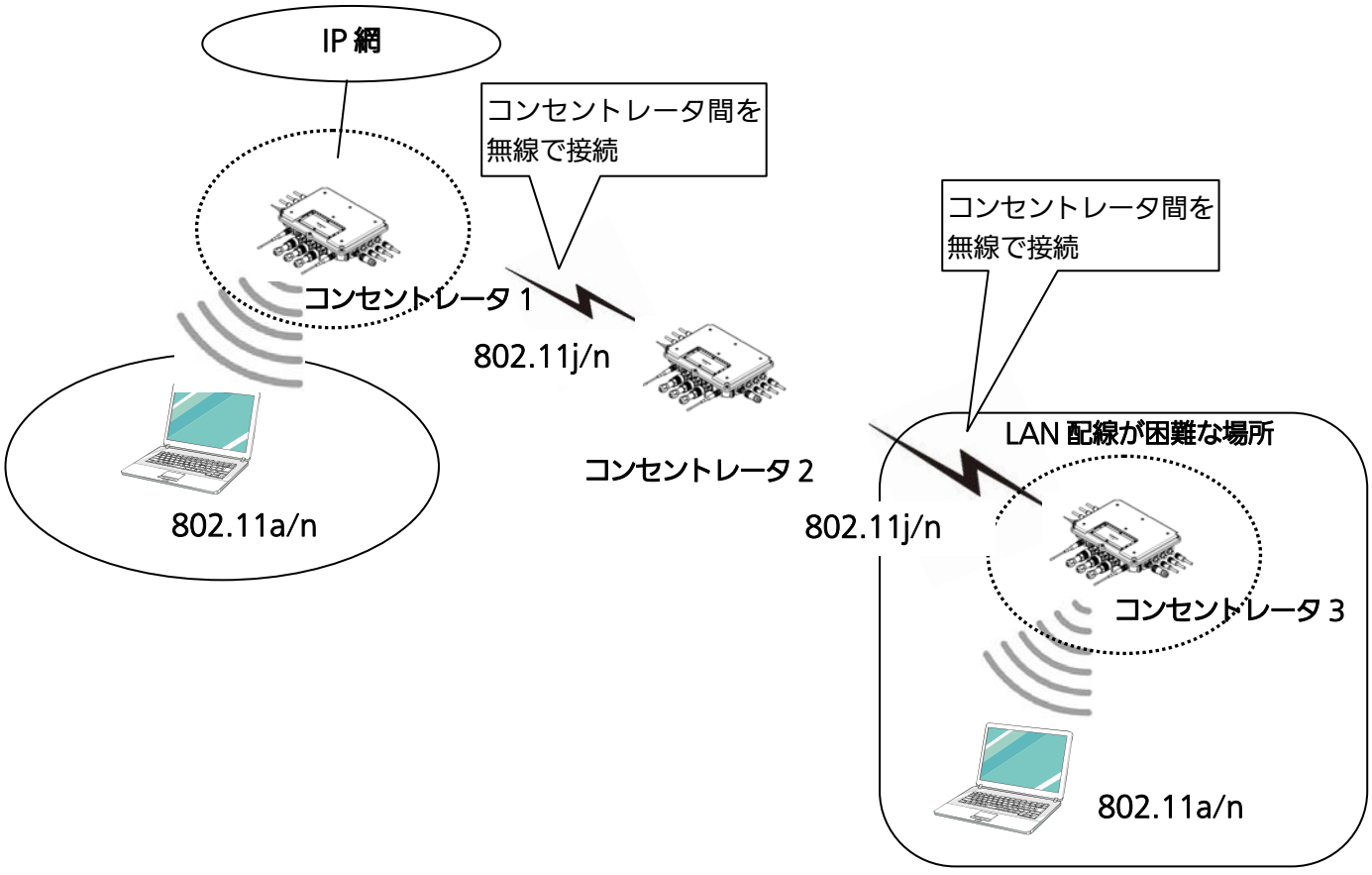


図1.2-1　　長距離通信イメージ

1.2.2.　多彩な Wi-Fi 基地局機能

コンセントレータの Wi-Fi 基地局機能では、2.4GHz（13ch）/5GHz（W56,11ch）のデュアルバンド、IEEE802.11n（3MIMO,450Mbps）に対応。さらに SSID 多重（最大 16）によるマルチサービスが可能となっています。

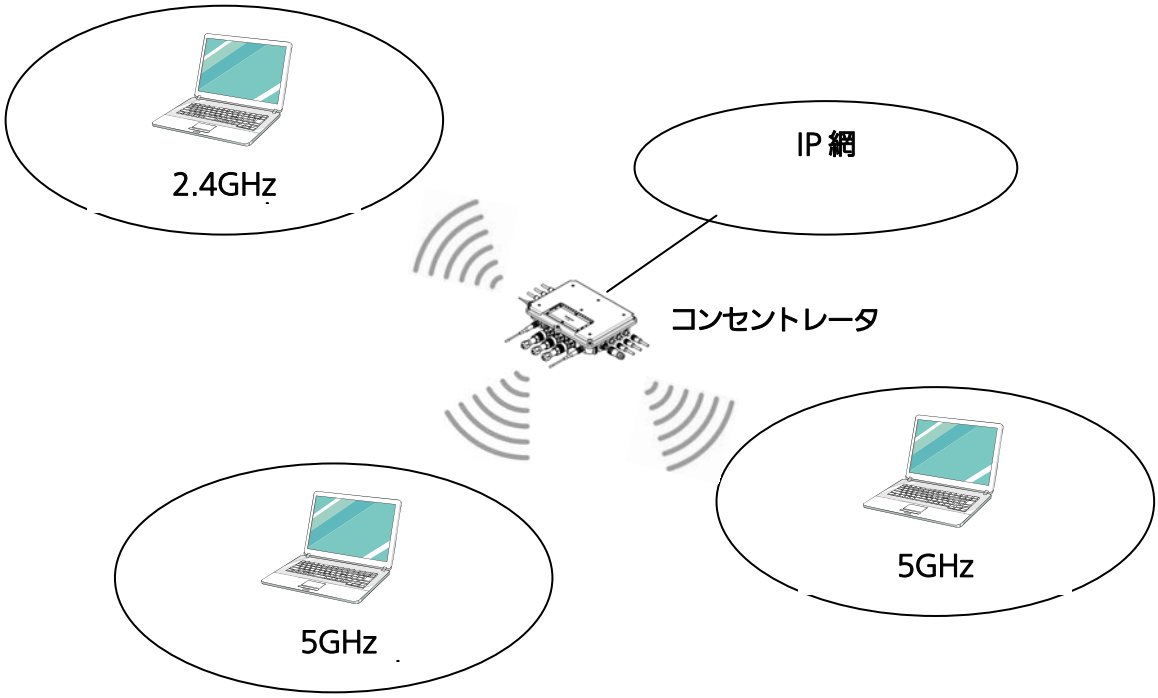


図1.2-2　多彩な Wi-Fi 基地局イメージ

1.2.3. マルチホップ通信に対応した 920MHz 帯通信機能

コンセントレータでは、マルチホップ通信に対応した 920MHz 帯 通信ユニットで各種センサ機器をオンライン化でき、コンセントレータ 1 台で 127 台の 920MHz 帯 通信ユニットの収容が可能です。

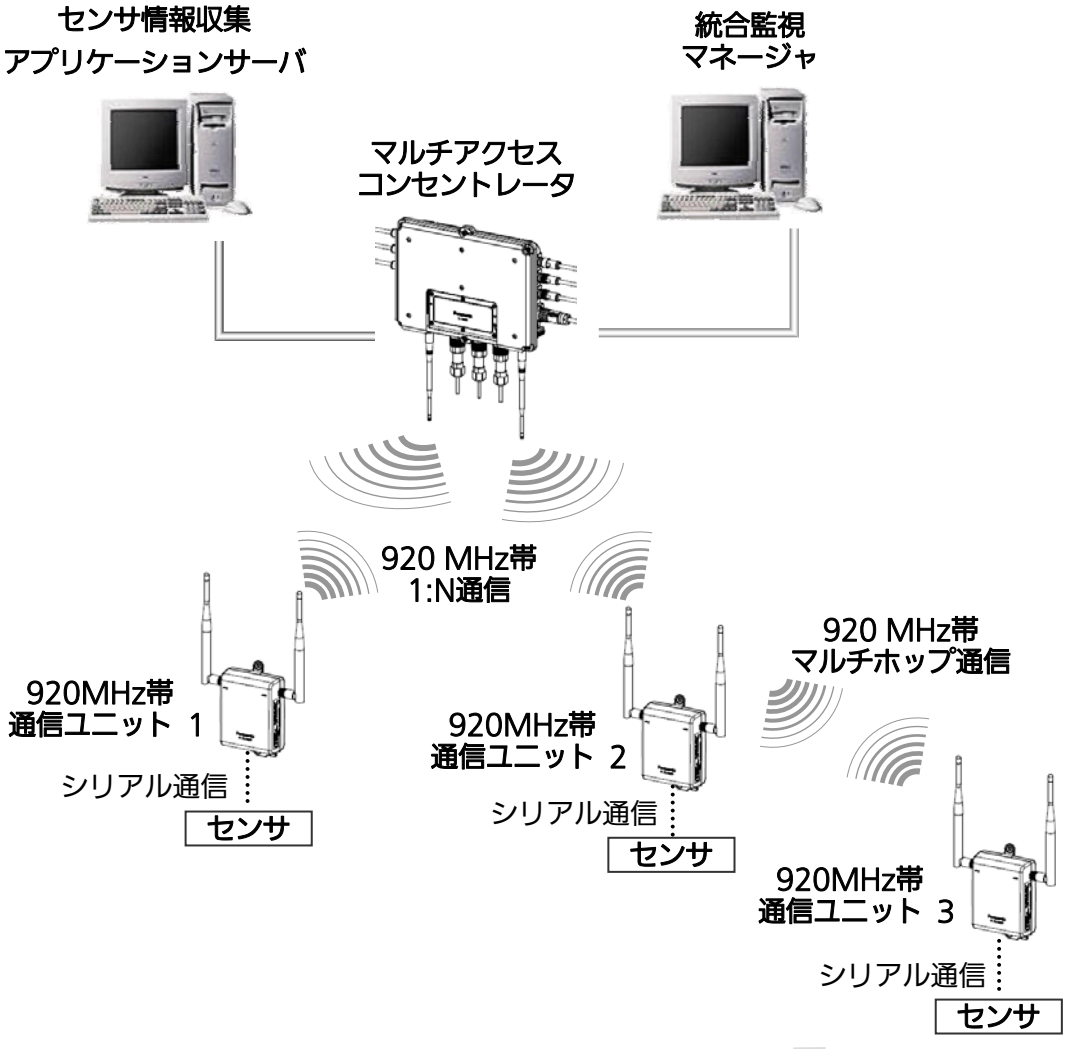


図1.2-3　マルチホップ 920MHz 帯通信イメージ

1.2.4.　450Mbps の高速伝送性

コンセントレータでは、802.11a/b/g に加えて、802.11n にも対応しています。802.11n では様々な規格が存在しますが、空間ストリーム数 3、伝送帯域幅 40MHz、ガードインターバル 400ns の 3 つの規格すべてに対応することで、5GHz 帯無線インターフェースで 450Mbps の伝送速度を実現しています。

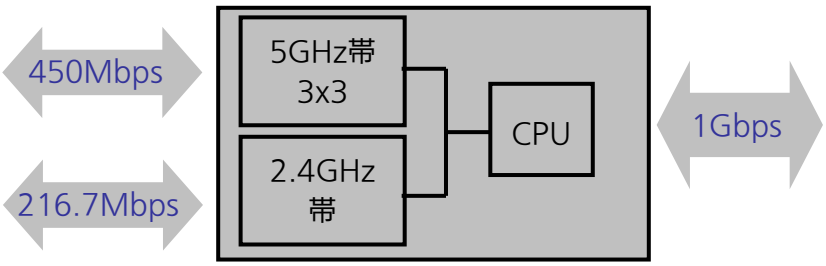


図1.2-4　ハードウェアイメージ

伝送速度の最高速は、規格による理論上の速度であり、ご利用環境や接続機器などにより実際のデータ速度は異なります。

1.2.5.　急増した無線 LAN 端末への対応　ー同時接続 320 台ー

スマートフォンを中心に無線 LAN 対応機器が急速に普及したため、1 台の無線 LAN アクセスポイント等への過密接続が問題となってきました。通信はほとんど行わないものの接続状態となったままの端末が増えることで、最大端末接続台数が数 10 台程度しかない従来の無線 LAN アクセスポイント等では、通信帯域に空きがあっても端末を追加接続することができませんでした。コンセントレータでは、無線 LAN インターフェースごとに最大 320 台の端末接続を実現し、また接続済の端末台数が一定以上の場合に限り、通信を行っていない端末を積極的に切断するなど、過密接続への課題に対応します。
ただし、同時通信台数を 320 台保証するわけではありません。

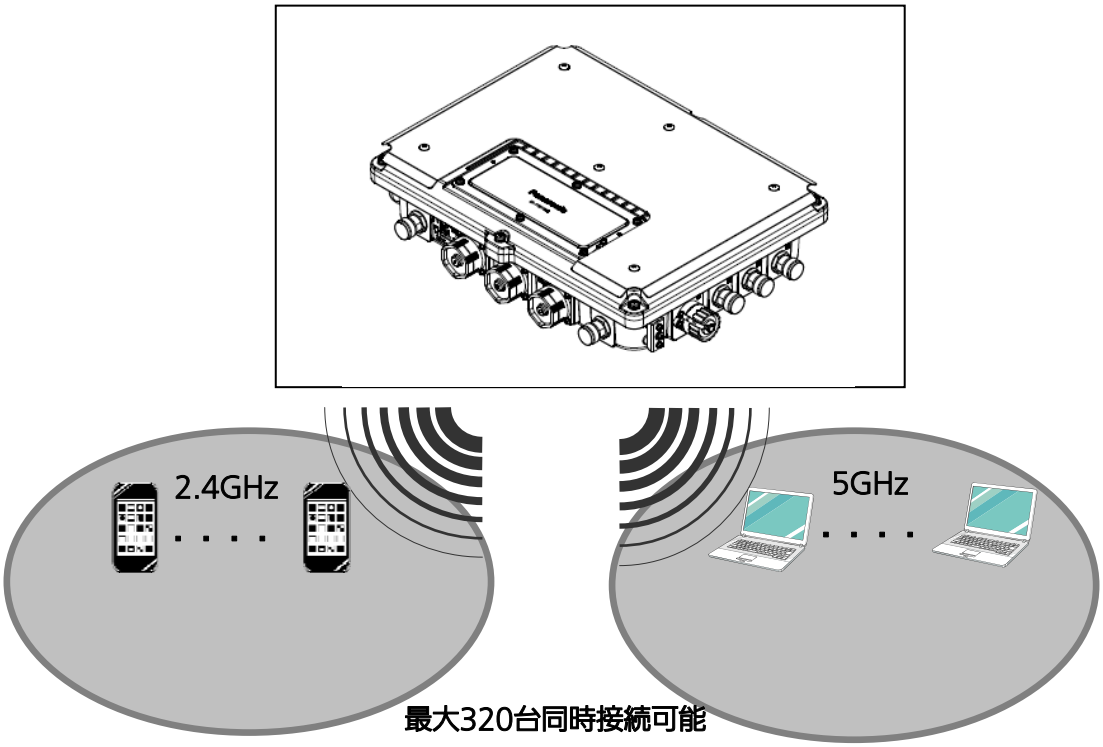


図1.2-5　同時接続イメージ

1.2.6. 各種 VPN ネットワークへの対応

コンセントレータを設置する場合、駅、飲食店、大規模商業施設などそれぞれの場所によって、アクセス網にも様々な形態が存在します。特にインターネット回線がすでに敷設されている場合は、L2TP＋IPsec のようなインターネット VPN 接続によりコンセントレータとセンター側ネットワークを結ぶことがあります。コンセントレータは VPN 機能を内蔵しており、機器コストや設置スペースに起因する運用コストの低減を可能にします。

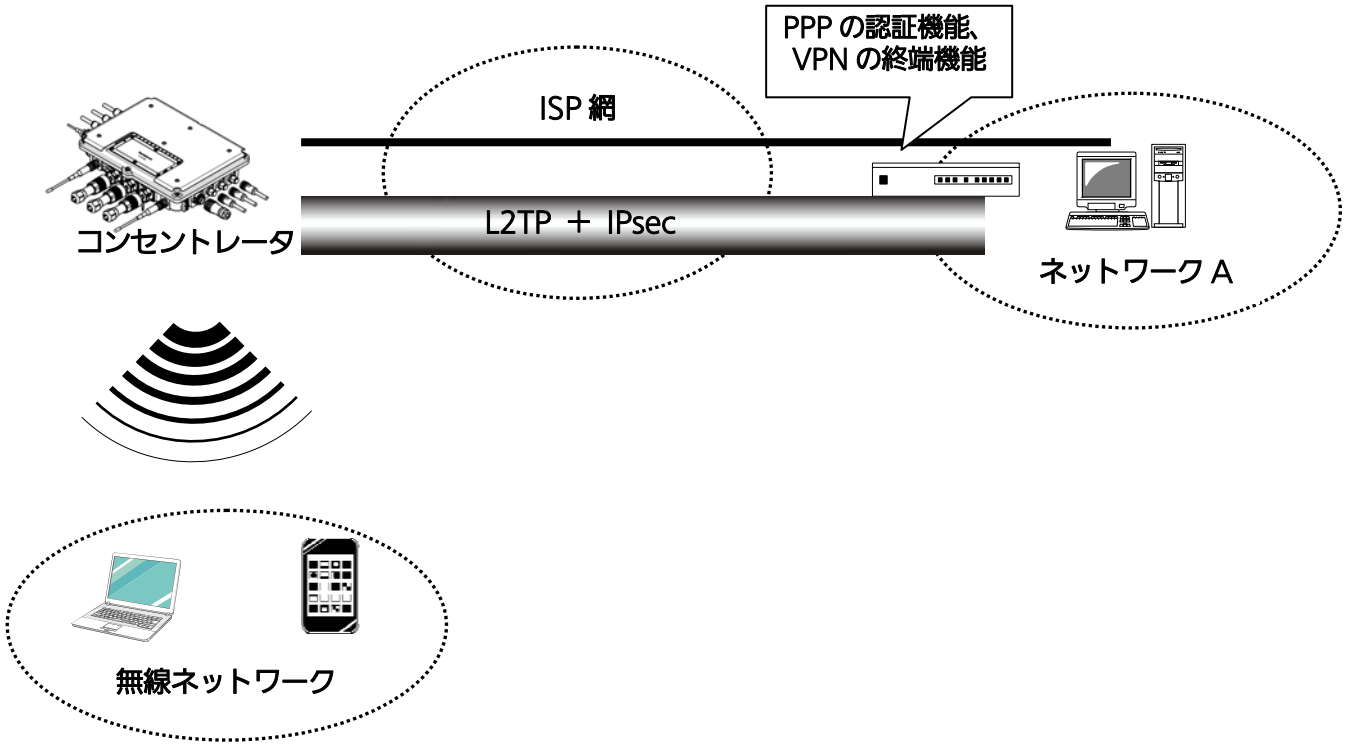


図1.2-6　VPN 接続イメージ

1.2.7. QoS（Quality of Service）機能

コンセントレータが備える QoS 機能は、大きく分けて優先制御と帯域制御の 2 つに分けられます。優先制御は、IP 電話など急ぎのパケットを、出力インターフェースでなるべく待たせずに送り出す技術です。一方の帯域制御は、特定の通信の帯域を確保したり、逆に制限したりする機能です。さらに、上記 2 つの機能を正しく利用するために、受け取った IP パケットを識別する機能を持ちます。これらの機能により、通信品質を保つことができます。

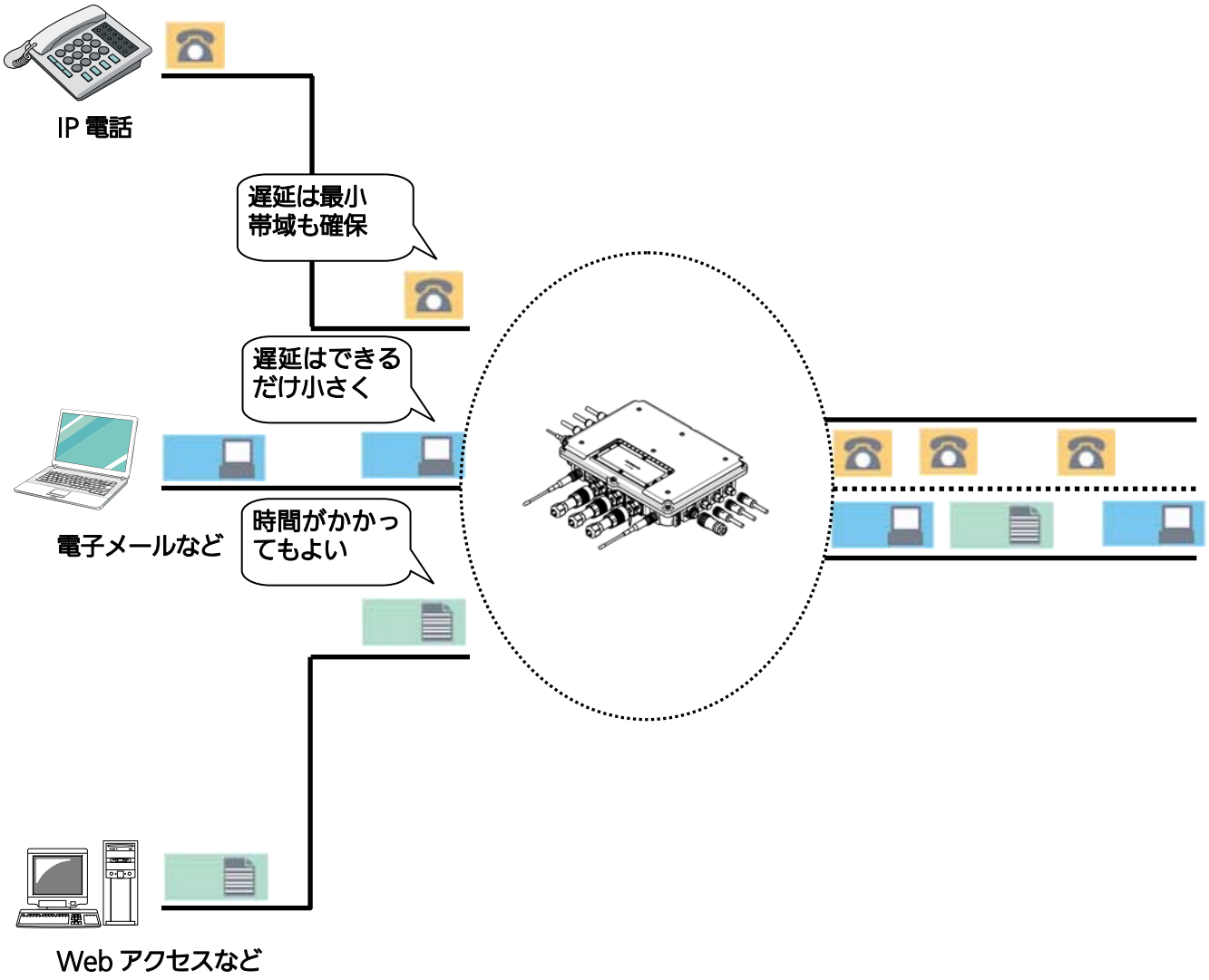


図1.2-7　QoS 機能イメージ

1.2.8. 端末接続制御機能

端末接続制御機能による、特定のコンセントレータへの端末接続集中を抑止します。SSID ごとに通信端末数の設定値をチューニングすることによって、たとえば、音声の通信要求が発生した際に、データ端末の接続を切断し、音声通信を優先させることができます。

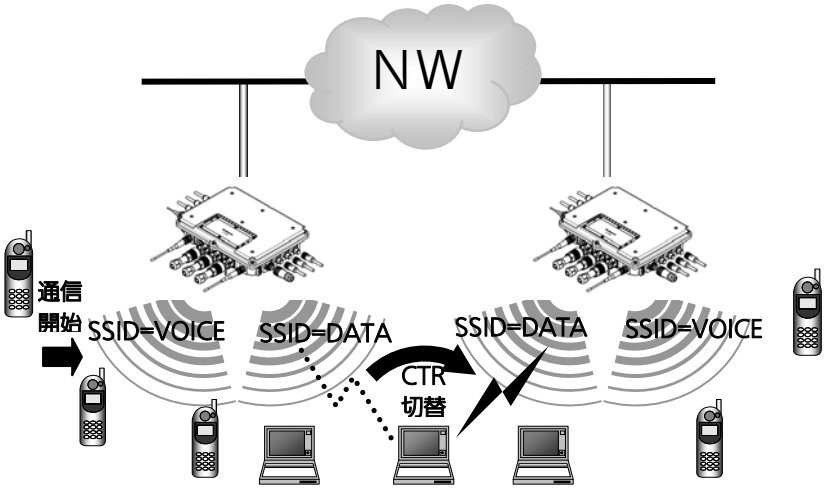


図1.2-8　端末接続制御機能イメージ

1.2.9. 無線ブリッジ機能

無線ブリッジ機能による、LAN 配線が困難な場所等に無線エリア拡張（コンセントレータ間を無線でつなぎます）が可能です。最大 64 分岐の多段接続に対応していますので、広域エリアへの適用も可能です。

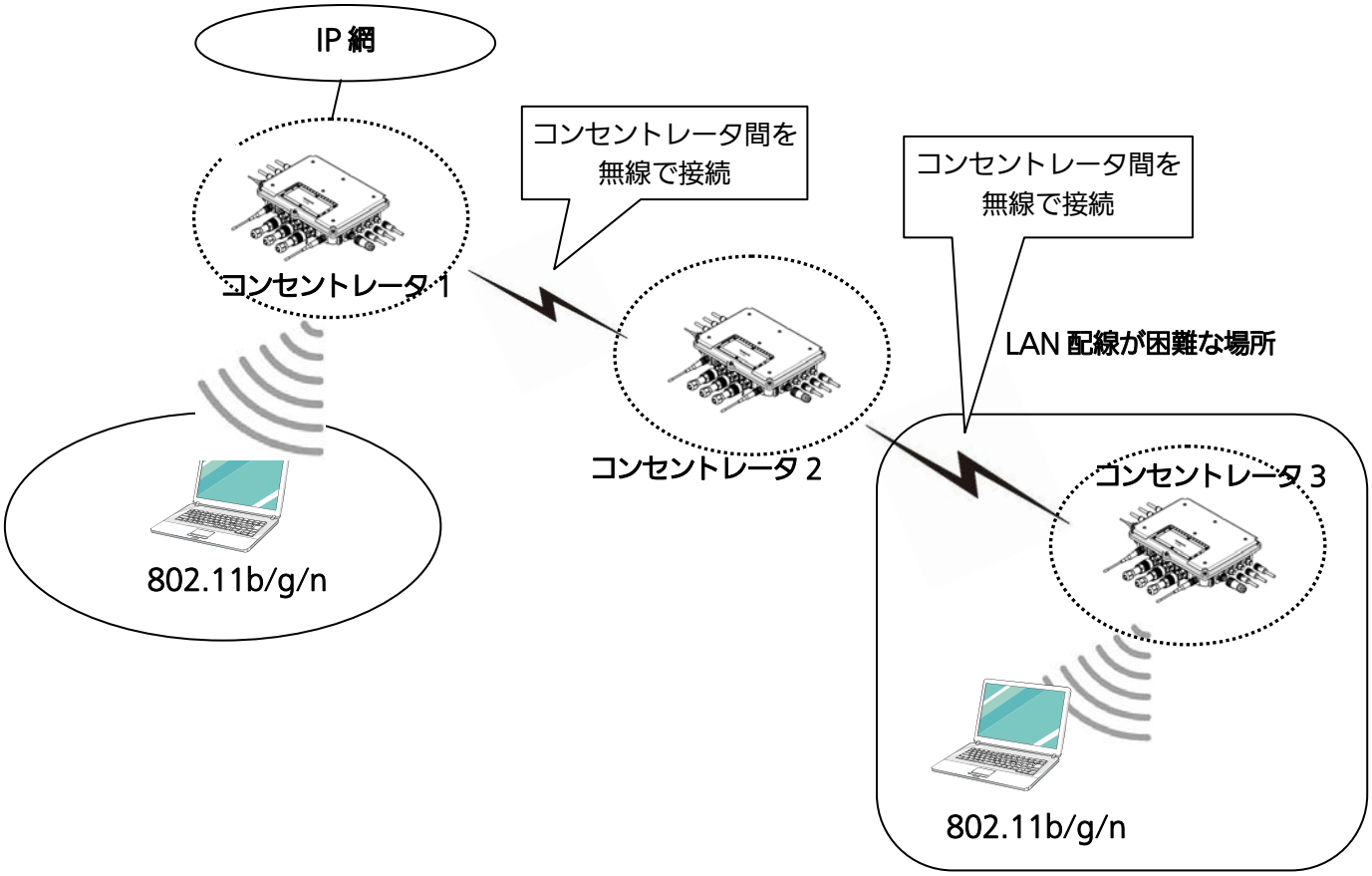


図1.2-9　無線ブリッジ機能イメージ

1.2.10.　多彩な VLAN（Virtual Local Area Network）機能

SSID ごとの VLAN 分離、ユーザ認証 VLAN に対応しています。

- SSID ごとに VLAN を設定することにより各 SSID のトラフィックを VLAN 分離可能です。
- 端末認証時の認証情報に従った、ユーザ認証 VLAN によりトラフィックを VLAN 分離可能です。
- SSID VLAN およびユーザ認証 VLAN を組み合わせたフレキシブルな VLAN 構成が可能です。

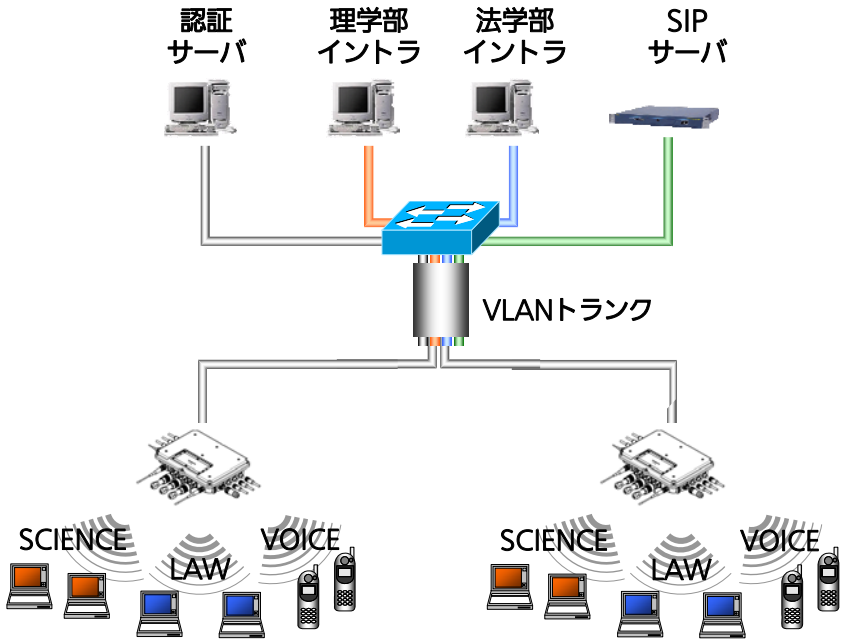


図1.2-10　VLAN 機能イメージ

1.2.11.　解析機能強化 ー統計情報管理・パケットログー

コンセントレータは、サービス事業者ごと（SSID 単位）に端末の接続状況やトラフィックなどのユーザ利用状況の把握が可能です。一定周期でアソシエーション成功／失敗の端末数、送受信したパケット数やバイト数などの情報を蓄積し、色々な分析や解析に利用できます。
また、アソシエーションから IEEE802.1X 認証完了までのコンセントレータ～端末間の接続シーケンスをパケットレベルで記録・保存する機能を持ち、接続問題の解析に活用できます。

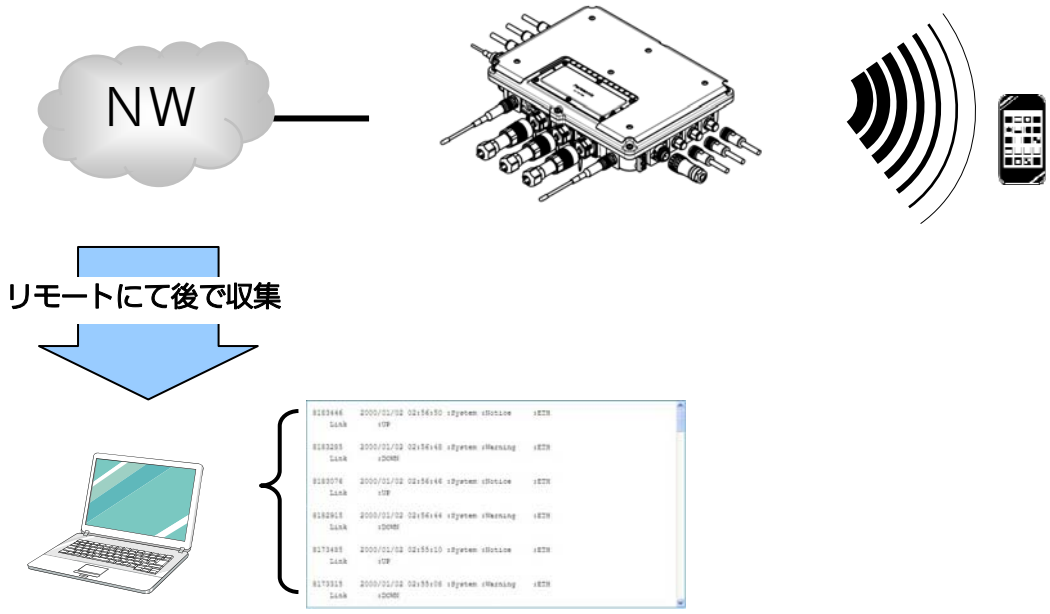


図 1.2-9　パケットキャプチャイメージ

1.2.12.　サービス品質向上の対応

コンセントレータではサービス品質向上のため、以下の機能も実装しております。

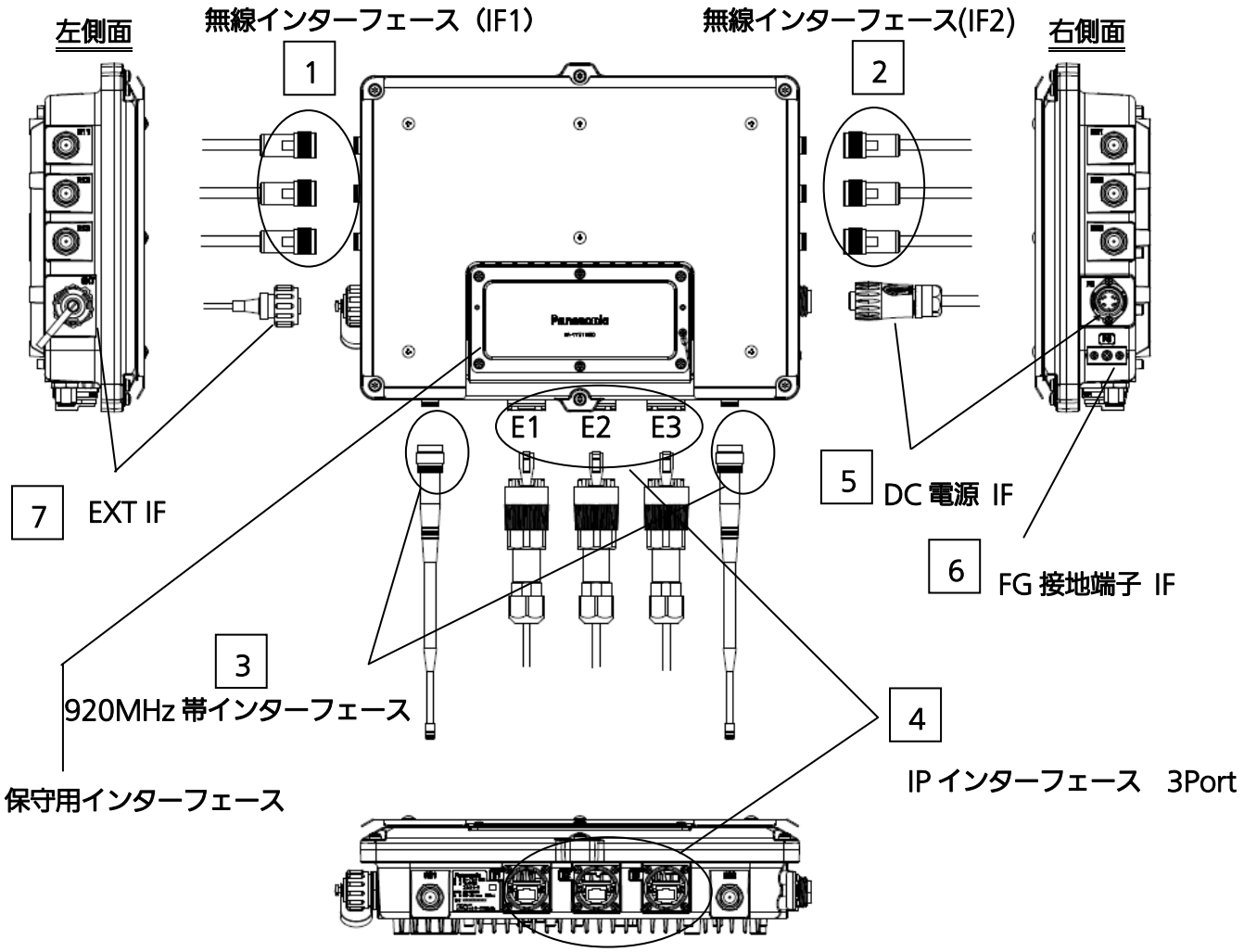
- 5GHz 帯域への誘導
- 低電界端末の接続拒否による、通信状態の安定化
- 同時端末接続数制御
- 最低接続保障台数制御
- IGMP スヌーピング
- Passpoint 対応

詳細は、4.7　サービス品質向上機能をご参照ください。

1.3　各部位の説明

1.3.1.　マルチアクセスコンセントレータ（EA-7TW11BS0）

外観、各部名称と機能について説明します。

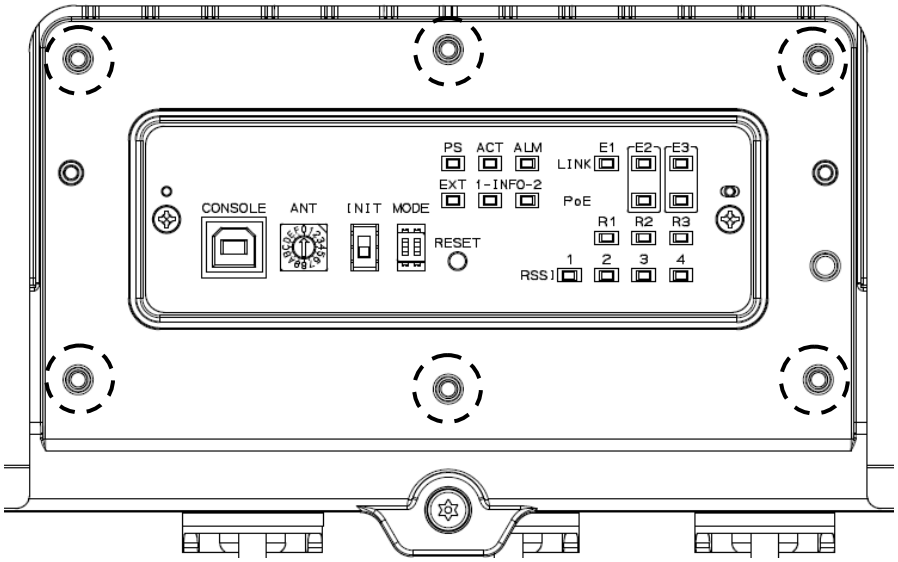


外部接続用のコネクタについて説明します。

外部接続コネクタ

番号	名　称	機　能
1	無線インターフェース（IF1） R11、R12、R13 (N コネクタジャック)	・無線 IF　#1（2.4G/5.6G/4.9 GHz）のアンテナ接続用同軸ケーブルを接続します。
2	無線インターフェース（IF2） R21、R22、R23 (N コネクタジャック)	・無線 IF　#2（2.4G/5.6G/4.9 GHz）のアンテナ接続用同軸ケーブルを接続します。
3	920MHz 帯インターフェース R31、R32 (N コネクタジャック)	・無線 IF　#3（920MHz）のアンテナもしくは、アンテナ接続用同軸ケーブルを接続します。
4	IP インターフェース　IF E1、E2、E3 （RJ-45 モジュラジャック）	Ethernet ケーブルを接続します。 左から 1 番です。 E1 ポートは PoE 給電装置から給電可能。 E2、E3 ポートは、PoE 給電に対応した外部装置に対して給電可能。 ※専用プラグを添付。
5	DC 電源　IF PS	DC-48V を接続します。 ※専用プラグを添付。
6	FG 接地端子　IF FG	FG と接続します。
7	EXT IF EXT （USB TYPE-A コネクタジャック）	USB 機器を接続します。（将来拡張用）

保守用インターフェースカバーを開けた際の　各 LED、スイッチ、コネクタについて説明します。



LED、スイッチ、コネクタ（1/2）

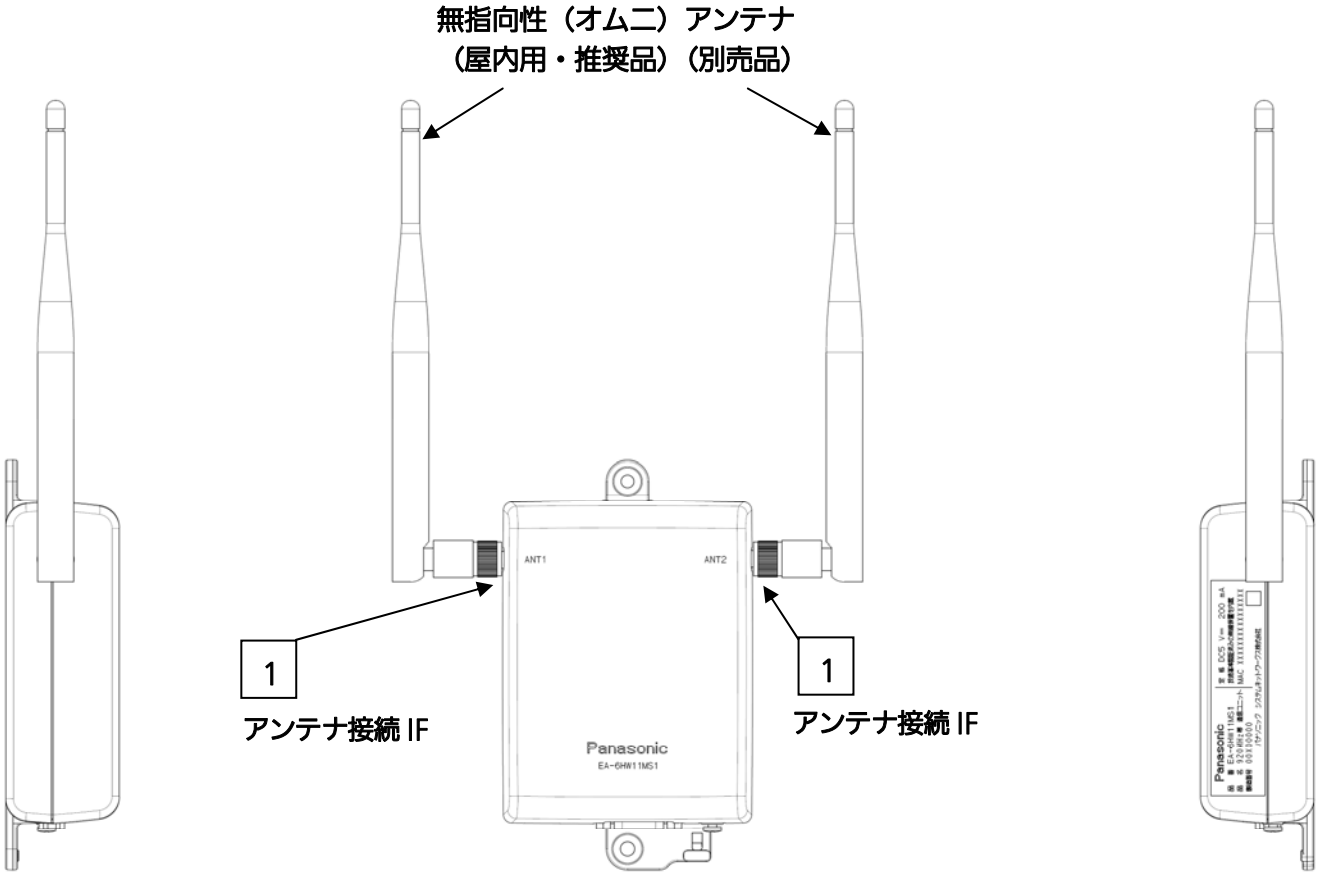
表　記	機　能	
PS （LED）	緑点灯	通電状態
	消灯	非通電状態
ACT （LED）	装置の運用状態を示します。	
	緑点灯	運用中
	緑点滅	・起動中 ・回線接続中 ・ダウンロード／アップロード中
	消灯	非通電状態、障害発生時
ALM （LED）	装置の障害状態を示します。	
	赤点灯	運用中の障害検出
	赤点滅	・INIT スイッチによる初期化実施 ・セルフテストにおいて障害が発生（状態は INFO［1:2］，RSSI[1:4]の LED を使用して示します）
	消灯	正常運用
LINK　E1、E2、E3 （LED）	Ethernet ポートのリンク状態を示します。（E1,E2,E3 の 3 ポート）	
	緑点灯	リンク確立・通信無し
	緑点滅	リンク確立・通信中
	消灯	リンク未確立
PoE　E2、E3 （LED）	Ethernet ポートの PoE 給電状態を示します。（E2,E3 の 2 ポート）	
	緑点灯	給電中
	緑点滅	PoE 関連異常：点滅(500 ms)
	消灯	給電停止中

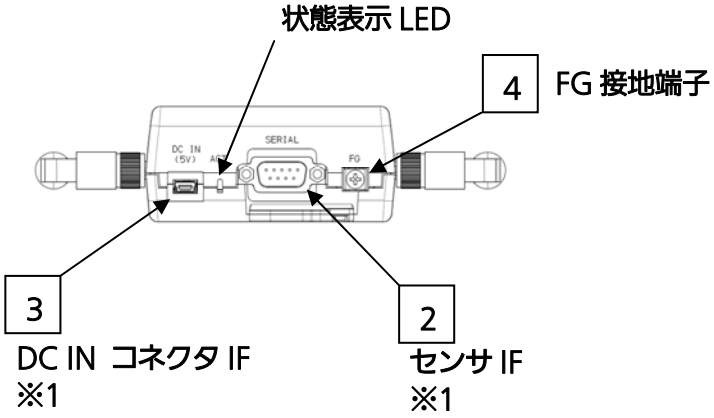
LED、スイッチ、コネクタ（2/2）

表　記	機　能	
R1 （LED）	無線 IF　＃1（2.4G/5.6G,4.9 GHz）の状態表示	
	緑点灯	通常運用中
	緑点滅	接続中
	消灯	起動中／閉塞状態
R2 （LED）	無線 IF　＃2（2.4 G/5.6 G,4.9 GHz）の状態表示	
	緑点灯	通常運用中
	緑点滅	接続中
	消灯	起動中／閉塞状態
R3 （LED）	無線 IF　＃3（920 MHz）の状態表示	
	緑点灯	通常運用中
	緑点滅	VerUP モード中
	消灯	起動中／閉塞状態／920M 無線出力停止時
RSSI　1、2、3、4 （LED）	WiFi 電波受信状態（RSSI）の表示。ロータリーSW（ANT）にて、表示するアンテナ系統を指定する。	
	緑点灯	受信レベルに応じて、4 段階点灯で状態表示
	緑消灯	
EXT （LED）	拡張用 USB ポートの状態表示	
	緑点灯	・通常運用中（TBD）
	緑点滅	・初期化中、接続中（TBD）
	消灯	・デバイス未接続（TBD）
INFO　1 （LED）	VPN 回線設定・接続の状態表示（USB 接続状態表示）	
	緑点灯	・VPN 設定済接続済み
	緑点滅	・VPN 設定済接続中：点滅(500ms)
	消灯	・未設定、未接続
INFO　2 （LED）	WAN 回線接続の状態表示	
	緑点灯	主回線接続
	緑点滅	副回線接続
	消灯	WAN 回線切断/回線冗長化設定無
ANT （ロータリースイッチ）	WiFi 電波受信状態（RSSI）を表示するアンテナ系統番号を指定する。 1：IF2、最大比合成後 2：IF2、アンテナ 0（R21） 3：IF2、アンテナ 1（R22） 4：IF2、アンテナ 2（R23） C：IF1、アンテナ 2 (R11) D：IF1、アンテナ 1 (R12) E：IF1、アンテナ 0 (R13) F：IF1、最大比合成後	
INIT （スライドスイッチ）	構成データ、ログデータを初期化します。 初期化の方法は 2.10 章をご参照ください。	
MODE　1、2 （スライドスイッチ）	コンセントレータでは使用しません。出荷状態から変更しないでください。	
RESET （プッシュスイッチ）	コンセントレータをリセットします。	
CONSOLE （USB TYPE-B コネクタジャック）	パソコンなど保守用のコンソールを接続します。	

1.3.2. 920MHz 帯 通信ユニット（EA-6HW11MS1）

外観、各部名称と機能について説明します。





※1 装置電源は、DC IN コネクタ IF またはセンサ IF から供給可能

外部接続用のコネクタについて説明します。

番号	表　示	名　称	機　能
1	ANT1/ANT2	アンテナ接続 IF	無線 IF（920 MHz 帯）アンテナ（またはアンテナ接続用同軸ケーブル）を接続します。
2	SERIAL	センサ IF	センサ IF ケーブルを接続します。
3	DC IN (5V)	DC IN コネクタ IF	DC +5 V を接続します。　※1
4	FG	FG 接地端子	FG 線を接続します。

LED の表示について説明します。

名　称	機　能	
状態表示 LED	装置の運用状態を示します。	
	緑点灯	運用中（リンク確立）
	緑点滅	・起動中 ・運用中（リンク確立前）
	赤点灯	重障害発生
	赤点滅	軽障害発生
	橙点灯	保守モード
	消灯	非通電状態

第 2 章　設定の準備

コンセントレータの設定のための準備について説明します。

2.1　Web コンソール用パソコンの設定

Web コンソールを利用する際に使用する、Web コンソール用パソコンの接続方法とコンセントレータの設定について説明します。

表2.1-1　Web コンソール用パソコンの推奨環境

OS および TCP/IP ソフトウェア	Microsoft® Windows® XP Microsoft® Windows Vista® Microsoft® Windows® 7 Microsoft® Windows® 8 TCP/IP ソフトウェアは OS に付属しています。別途ご用意いただく必要はありません。
画面解像度	1024 x 768 ピクセル以上
LAN カード	コンセントレータとパソコンを接続するために、パソコンに Ethernet ポートが必要です。LAN カードを使用する場合は、ご使用になるパソコンに装着できる LAN カードをご用意ください。
WWW ブラウザ	コンセントレータの設定に Web コンソールを使用する際には、以下の WWW ブラウザをご用意ください。 ・Windows® Internet Explorer 8.0®以上 ※同一端末で複数ブラウザ画面からのアクセスには対応しておりません。

◆LAN カードの準備

Web コンソール用パソコンに Ethernet ポートがあることを確認してください。Ethernet ポートがないパソコンの場合は、LAN カードを装着する必要があります。LAN カードを新規に装着した場合には、LAN カードのソフトウェア（ネットワークドライバ）のインストールが必要となります。パソコンや LAN カードに添付されたマニュアルに従って正しく設定してください。

◆TCP/IP プロトコルの設定

Web コンソールを使用するには、Web コンソール用パソコンで IP アドレスおよびサブネットマスクの設定を済ませておくことが必要です。
設定の手順はパソコンの OS によって異なります。本書では、Microsoft® Windows® 8 を例に説明します。

パソコンの TCP/IP の設定を行います。

設定手順

手順1　〔コントロールパネル〕ウインドウを開き、表示方法がカテゴリの場合〔ネットワークとインターフネット〕を開き、〔ネットワークと共有センター〕をクリックします。

手順2　〔アダプターの設定の変更〕をクリックします。〔イーサネット〕が表示されます。

手順3　〔イーサネット〕をダブルクリックします。〔イーサネットのプロパティ〕ダイアログボックスが表示されます。

手順4　一覧にインターネット プロトコル バージョン 4 (TCP/IPv4) が含まれていることを確認します。
一覧にインターネット プロトコル バージョン 4（TCP/IPv4）が表示されていない場合は、TCP/IP のインストールが必要です。Microsoft® Windows® 8 のマニュアルを参照して、インストールしてください。

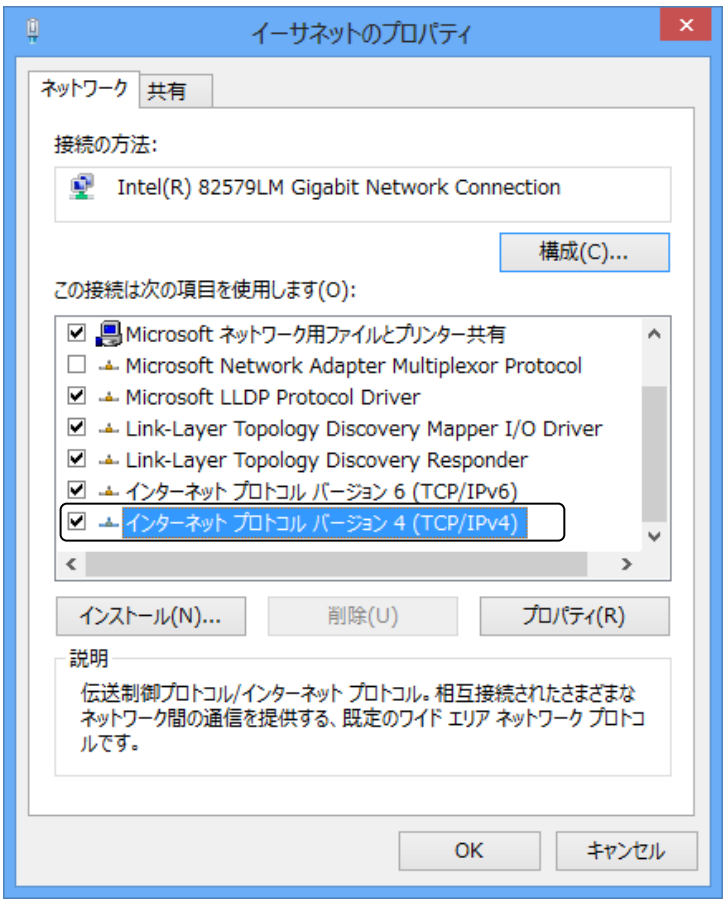


図2.1-1　イーサネットのプロパティ

手順5　一覧から〔インターネット プロトコル バージョン 4 (TCP/IPv4)〕をクリックして選択し、〔プロパティ〕をクリックします。

手順6　パソコンの IP アドレスを設定します。設定する IP アドレスとサブネットマスクは、コンセントレータに設定されている IP アドレスとサブネットマスクと整合性をとるように設定してください。コンセントレータの IP アドレスの初期値は、表 2.1-2 に記載します。

表2.1-2　IP アドレス（初期値）

IP アドレス	192.168.0.3
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.0.1

例として、下記内容での設定を示します。

- 〔次の IP アドレスを使う〕を選択
- IP アドレスに「192.168.0.10」を入力
- サブネットマスクに「255.255.255.0」を入力
- デフォルトゲートウェイは入力なし

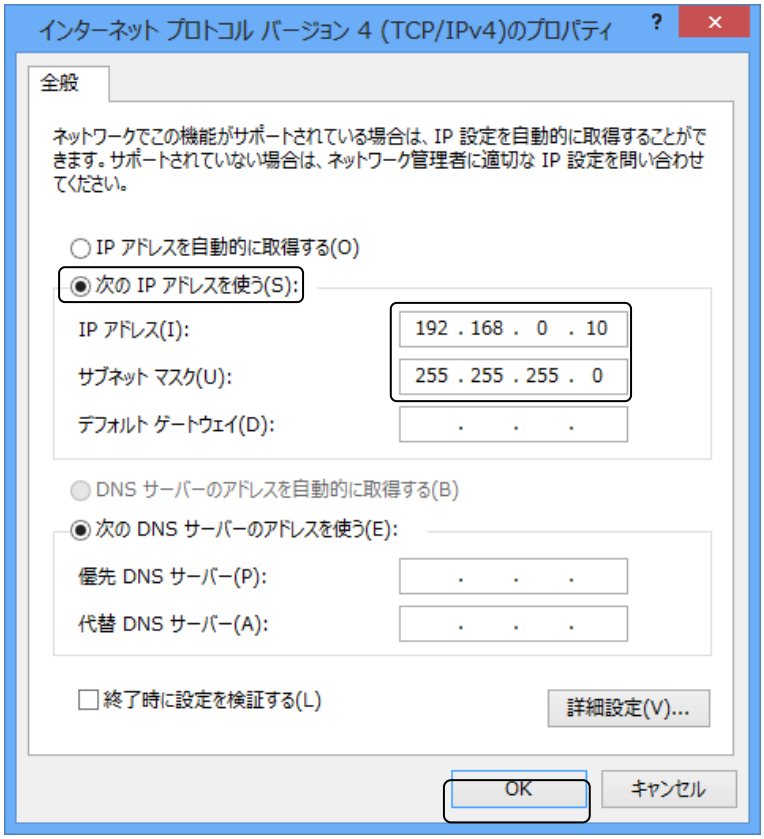


図2.1-2　インターネット プロトコル バージョン 4（TCP/IPv4）のプロパティ

手順7　〔OK〕をクリックして、〔イーサネットのプロパティ〕に戻ります。
手順8　〔閉じる〕をクリックして、〔イーサネットの状態〕に戻ります。
手順9　〔閉じる〕をクリックします。

◆Web ブラウザの準備

設定の手順はパソコンの OS によって異なります。本書では、Microsoft® Windows® 8 を例に説明します。

設定手順

手順1　〔コントロールパネル〕ウインドウを開き、表示方法がカテゴリの場合〔ネットワークとインターフネット〕を開き、〔インターネットオプション〕をクリックします。〔インターネットのプロパティ〕ダイアログボックスが表示されます。

手順2　〔接続〕タブを選択し、〔LAN の設定〕をクリックします。

手順3　〔プロキシサーバを使用する〕がチェックされていないことを確認します。

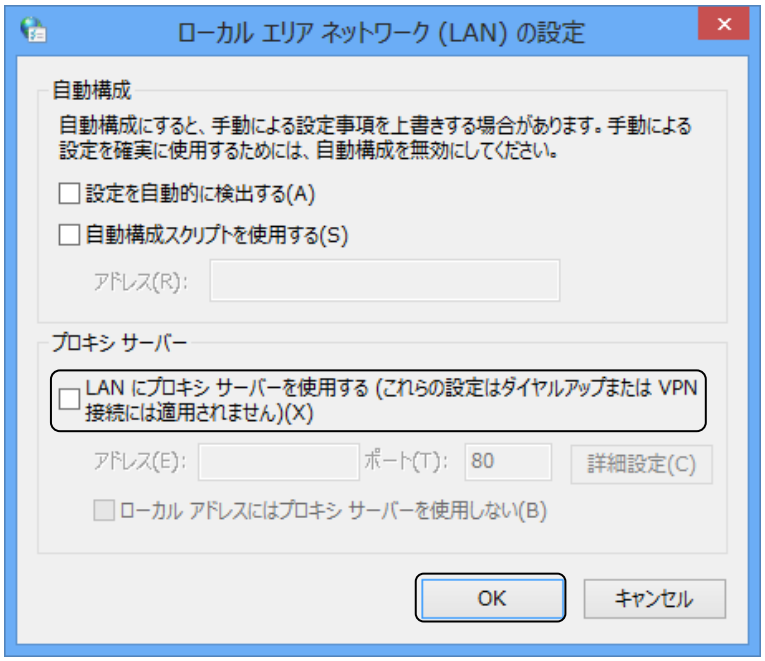


図2.1-3　ローカルエリアネットワークの設定（LAN）

プロキシサーバを利用する場合は、コンセントレータだけプロキシの対象外として設定してください。

手順4　〔コントロールパネル〕ウインドウを開き、〔インターネットオプション〕をクリックします。〔インターネットのプロパティ〕ダイアログボックスが表示されます。

手順5　〔接続〕タブを選択し、〔LAN の設定〕をクリックします。

手順6　〔LAN にプロキシサーバを使用する〕をチェックし、〔詳細設定〕をクリックします。

手順7　例外の〔次で始まるアドレスにはプロキシを使用しない〕にコンセントレータの IP アドレスを指定します。

手順8　〔OK〕をクリックして、〔ローカルエリアネットワーク（LAN）の設定〕に戻ります。

手順9　〔OK〕をクリックして、〔インターネットのプロパティ〕に戻ります。

手順10　〔OK〕をクリックします。

2.2　Web でのログイン・ログアウト

◆ユーザ種別

ユーザアカウントには、管理ユーザと一般ユーザの 2 種類があります。それぞれについては、表 2.2-1 にまとめています。

表2.2-1　ユーザ種別

	ユーザ名	パスワード	権限
管理ユーザ	root	root	すべての操作が可能
一般ユーザ	user	user	設定や状態の表示のみ可能

重要	■ ユーザ名・パスワードは初期値の設定から必ず変更し、適正に管理してください。ユーザ名・パスワードの変更方法については、「2.3 ユーザ名・パスワードの変更」を参照してください。

◆ログイン

Web ブラウザに表 2.1-2 の IP アドレスを入力すると、ログイン画面（図 2.2-1）が表示されます。
ユーザ種別（表 2.2-1）のユーザ名とパスワードを入力してください。

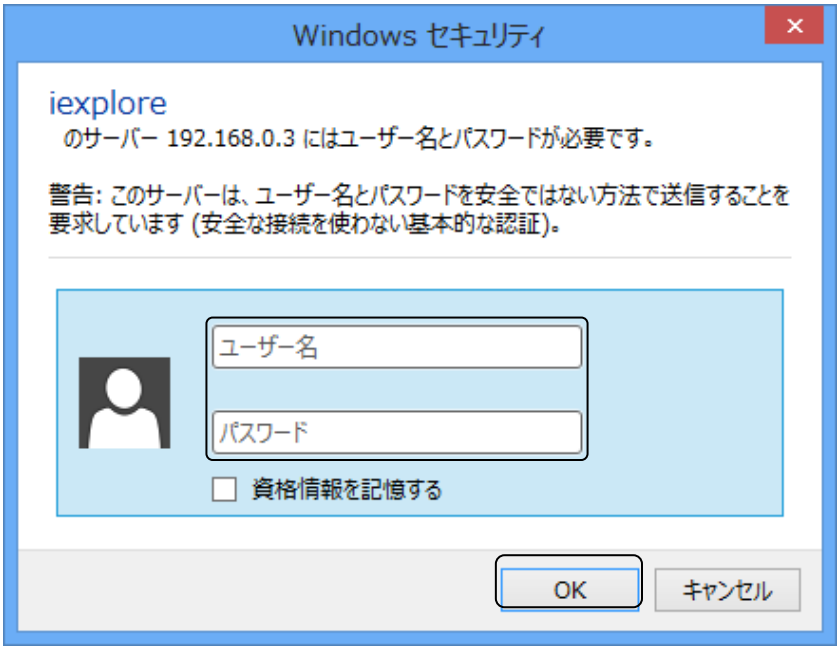


図2.2-1　ログイン画面

ユーザ名とパスワードが正しい場合、Web コンソールメイン画面（図 2.2-2）が表示され、該当するユーザレベルでのコンソール操作が可能となります。
また、コンセントレータのアカウントは、ユーザ権限に関わらず、1 つのアカウントのみ使用できます。
なお、Web コンソールメイン画面のレイアウトが乱れる場合には、互換表示で使用してください。

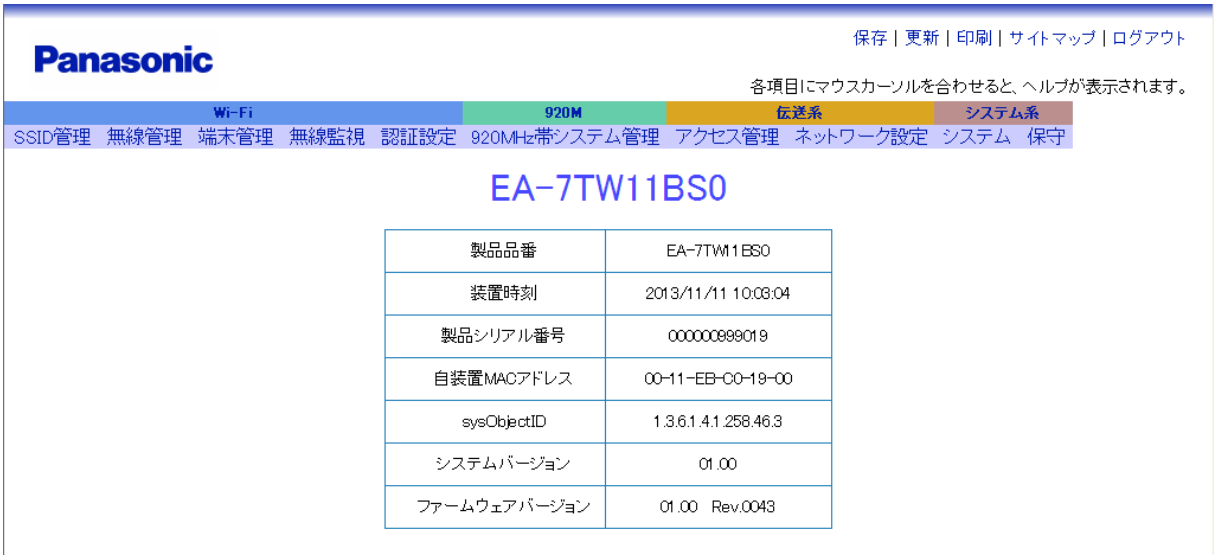


図2.2-2　Web コンソールメイン画面

◆ログアウト
Web コンソール画面の右上の〔ログアウト〕をクリックしてください。

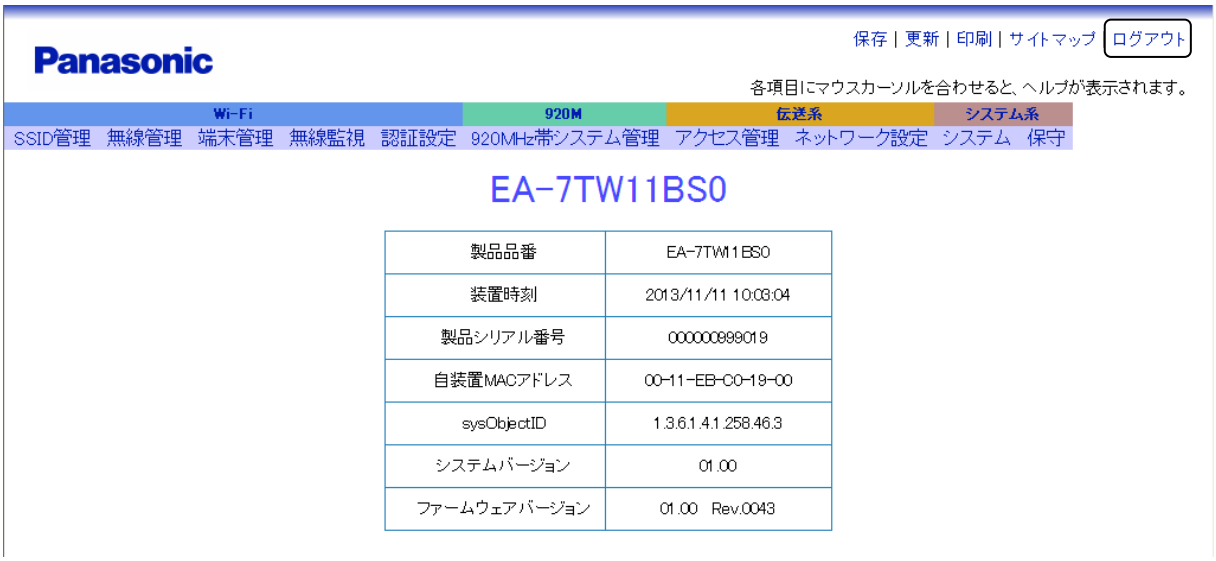


図2.2-3　Web コンソールメイン画面（ログアウト）

画面を閉じるか確認するダイアログが表示されますので、〔はい〕を選択して画面を閉じてください。

また、IP の変更を行った場合自動でログアウトされます。

2.3　ユーザ名・パスワードの変更

コンセントレータへのログインに必要なアカウント情報（ユーザ名・パスワード）は、それぞれ[ユーザ名：0～16 文字（英・数字）] 、[パスワード：0～16 文字（英・数字）]にて設定することができます。

◆ユーザ名変更

Web コンソールでのユーザ名の変更に関する設定は以下の通りです。ユーザを変更する場合は、管理ユーザでログインする必要があります。

設定手順

手順1　〔システム系〕　→　〔保守〕　→　〔ユーザ名変更〕を選択します。

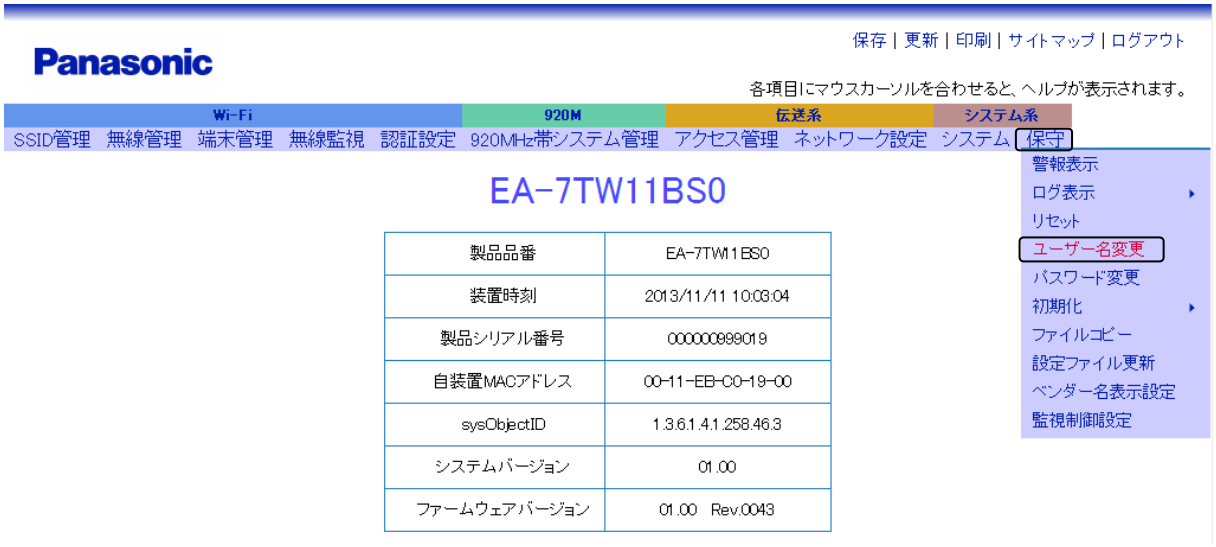


図2.3-1　メニュー（ユーザ名変更）

手順2　ユーザ名を変更します。

例として、下記内容での設定を示します。

- ユーザ種別：〔一般ユーザ〕を選択
- ユーザ名：「user01」を入力

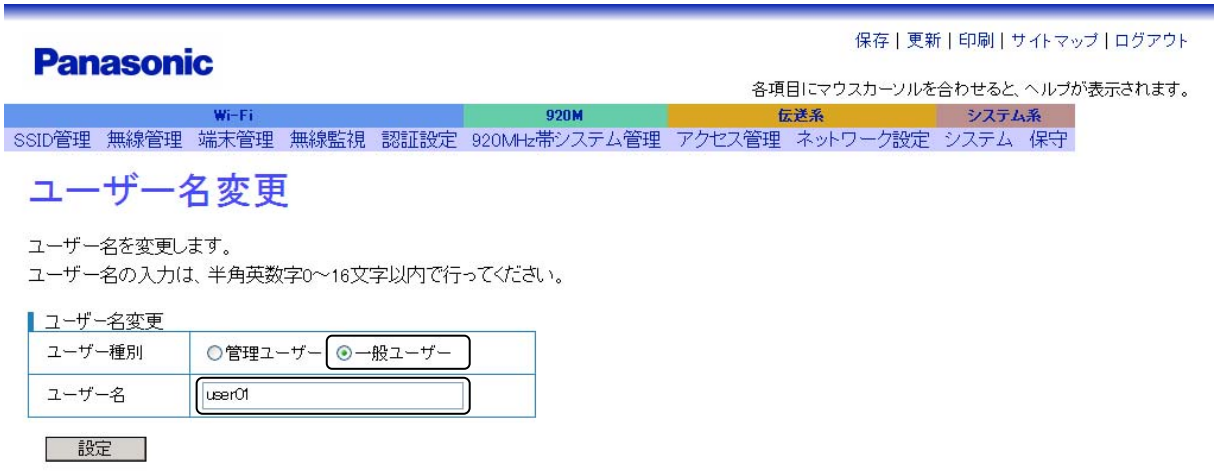


図2.3-2　ユーザ名変更

手順3　編集が完了したら、〔設定〕をクリックします。

◆パスワード変更

Web コンソールでのパスワードの変更に関する設定は以下の通りです。

手順1　〔システム系〕　→　〔保守〕　→　〔パスワード変更〕を選択し、パスワードを変更します。

例として、下記内容での設定を示します。

・　ユーザ種別：〔一般ユーザ〕を選択

・　古いパスワード～新しいパスワード（確認用）を入力

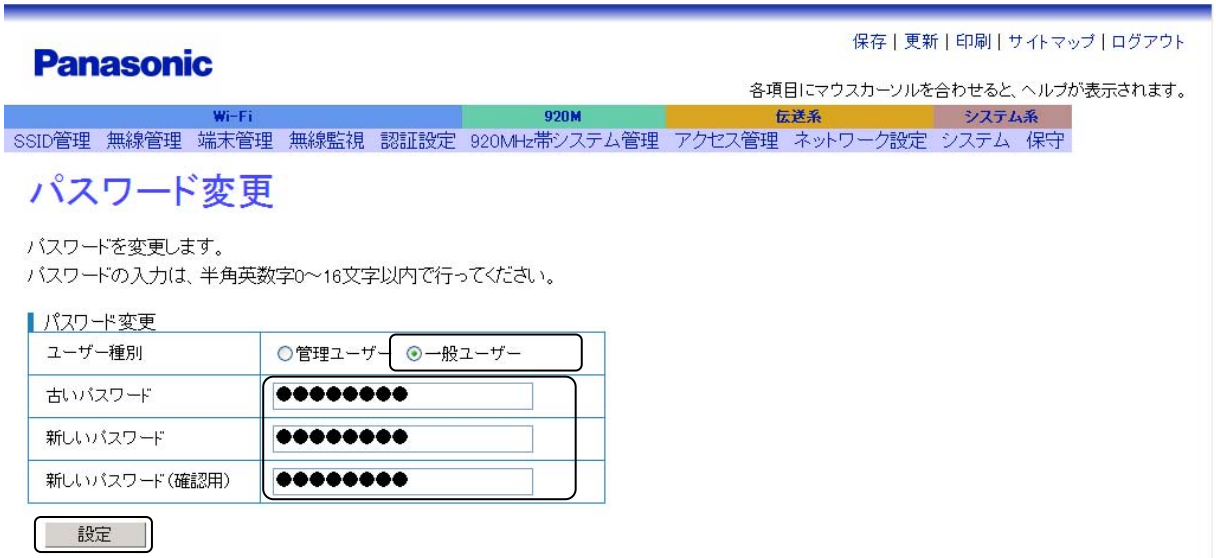


図2.3-3　パスワード変更

手順2　編集が完了したら、〔設定〕をクリックします。

重要	■ ユーザ名およびパスワードを変更する場合、管理ユーザでログインしておく必要があります。 ■ 管理ユーザのアカウント情報は、厳重に管理願います。管理ユーザのアカウント情報がわからなくなった場合、ログインによる再設定ができません。 ■ セキュリティ上、初期設定時は「管理ユーザ」「一般ユーザ」のアカウント情報を変更するようお願いいたします。

2.4　CLI コンソールでのログイン・ログアウト

コンセントレータの各種設定を行う方法には、Web コンソールのほかに、CLI コンソール（コマンドライン・インターフェース・コンソール）があります。ここでは、CLI コンソールの準備、ログイン・ログアウト方法について説明します。

◆コンソールの接続方法

コンソールとは、通信ソフトがインストールされているパソコンなどを指します。コンセントレータとコンソールを接続するには、USB ケーブルでコンソールポートとシリアル接続する方法と、Ethernet ケーブルで接続し、ネットワーク経由で Telnet によりリモートログインする方法があります。USB ケーブルで接続する場合、あらかじめコンソール用 PC にドライバをインストールしておく必要があります。ドライバはパナソニックビジネスサイト（http://panasonic.biz/netsys/wifi）からダウンロードしてください。

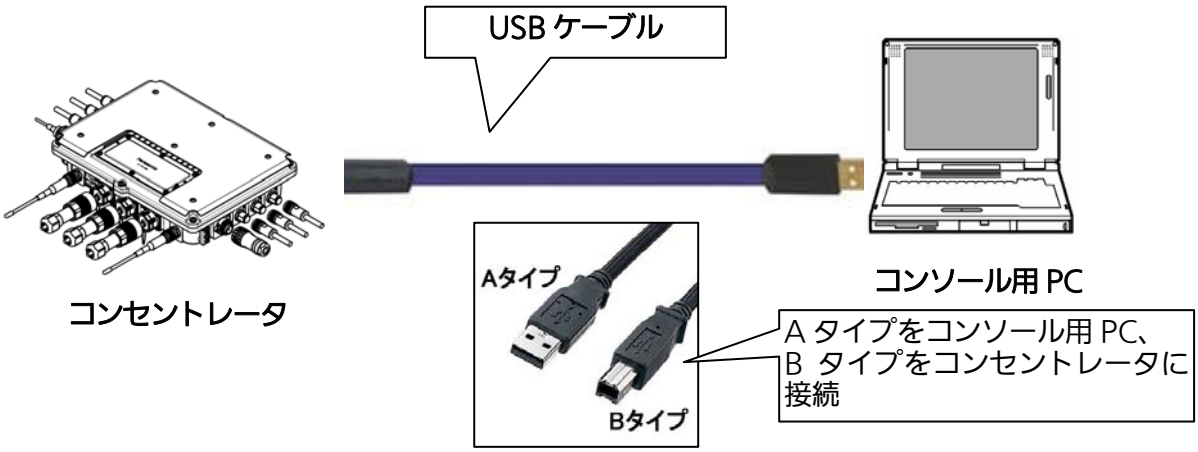


図2.4-1　コンソール接続例（USB ケーブル）

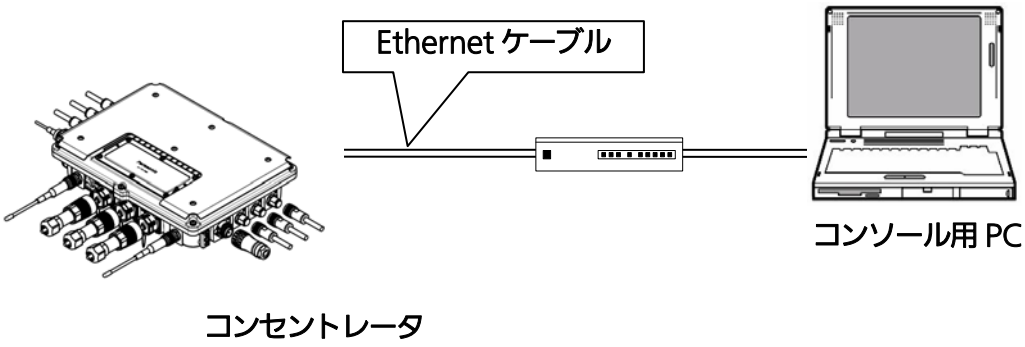


図2.4-2　コンソール接続例（Telnet）

◆USB ドライバインストール手順
本書では、Microsoft® Windows® 8 を例に説明します。
※コンソール用 PC に以下の権限のユーザでログインしてください。
Microsoft® Windows® 7/ Microsoft® Windows Vista®：「管理者」権限をもつユーザ
Microsoft® Windows® XP：「コンピュータの管理者」権限をもつユーザ

手順1　ダウンロードしたファイルをダブルクリックします。〔ユーザー アカウント制御〕画面が表示されるので〔はい（Y）〕をクリックします。その後、〔InstallShield Wizard〕画面が表示されるので〔Next > 〕をクリックします。

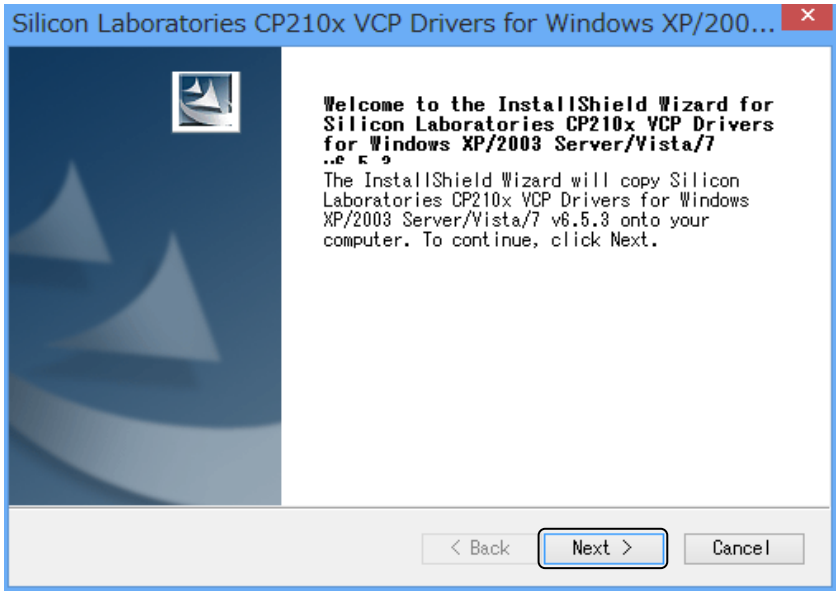

Silicon Laboratories CP210x VCP Drivers for Windows XP/200...
Welcome to the InstallShield Wizard for Silicon Laboratories CP210x VCP Drivers for Windows XP/2003 Server/Vista/7
The InstallShield Wizard will copy Silicon Laboratories CP210x VCP Drivers for Windows XP/2003 Server/Vista/7 v6.5.3 onto your computer. To continue, click Next.
< Back
Next >
Cancel

図2.4-3　InstallShield Wizard

手順2　〔License Agreement〕画面が表示されます。ライセンス条件をご確認のうえ、〔I accept the terms of the license agreement〕をクリックし、〔Next > 〕をクリックします。

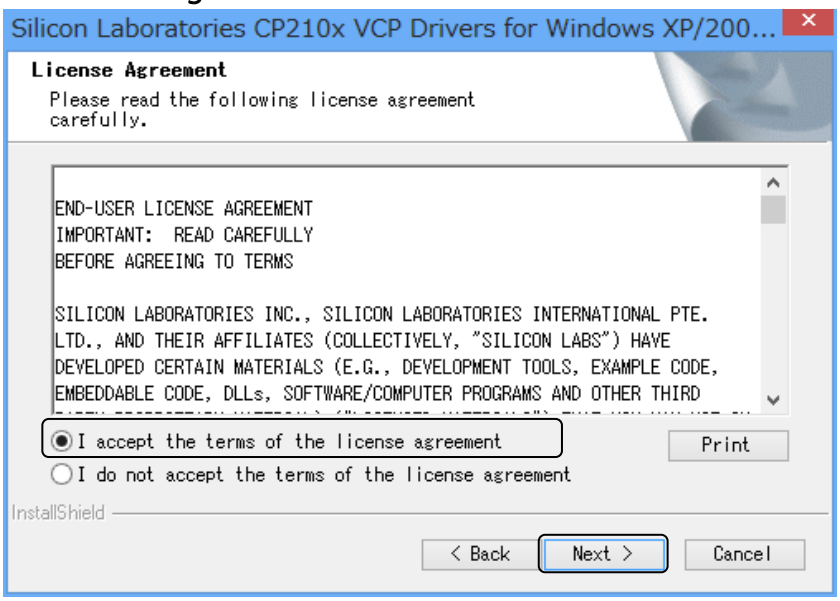

Silicon Laboratories CP210x VCP Drivers for Windows XP/200...
License Agreement
Please read the following license agreement carefully.
END-USER LICENSE AGREEMENT
IMPORTANT: READ CAREFULLY
BEFORE AGREEING TO TERMS
SILICON LABORATORIES INC., SILICON LABORATORIES INTERNATIONAL PTE. LTD., AND THEIR AFFILIATES (COLLECTIVELY, "SILICON LABS") HAVE DEVELOPED CERTAIN MATERIALS (E.G., DEVELOPMENT TOOLS, EXAMPLE CODE, EMBEDDABLE CODE, DLLs, SOFTWARE/COMPUTER PROGRAMS AND OTHER THIRD
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

図2.4-4　License Agreement

手順3　〔Choose Destination Location〕画面が表示されるのでインストール先のディレクトリを変更する場合は〔Browse...〕をクリックしインストール先を指定後、〔Next > 〕をクリックします。

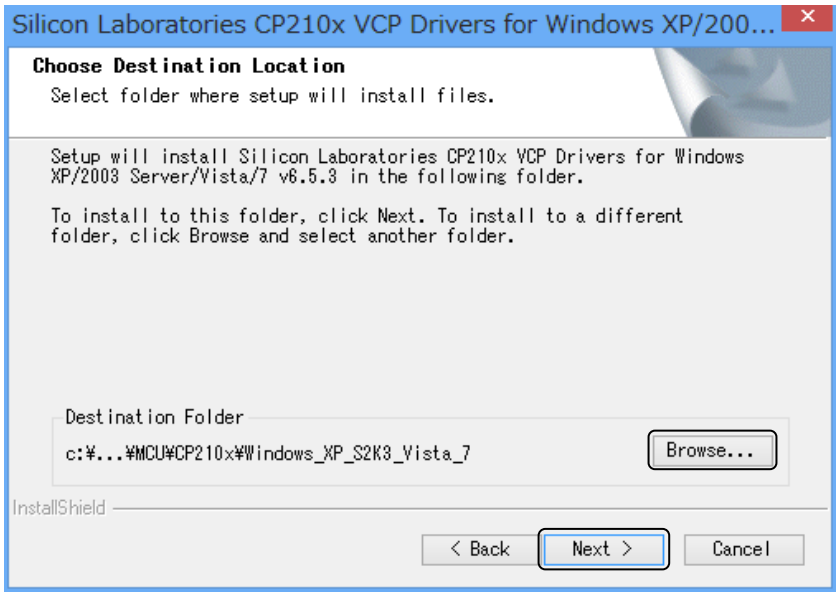

Silicon Laboratories CP210x VCP Drivers for Windows XP/200...
Choose Destination Location
Select folder where setup will install files.
Setup will install Silicon Laboratories CP210x VCP Drivers for Windows XP/2003 Server/Vista/7 v6.5.3 in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
c:¥...¥MCU¥CP210x¥Windows_XP_S2K3_Vista_7
Browse...
InstallShield
< Back
Next >
Cancel

図2.4-5　Choose Destination Location

手順4　〔Ready to Install the Program〕画面が表示されるので〔Install〕をクリックします。

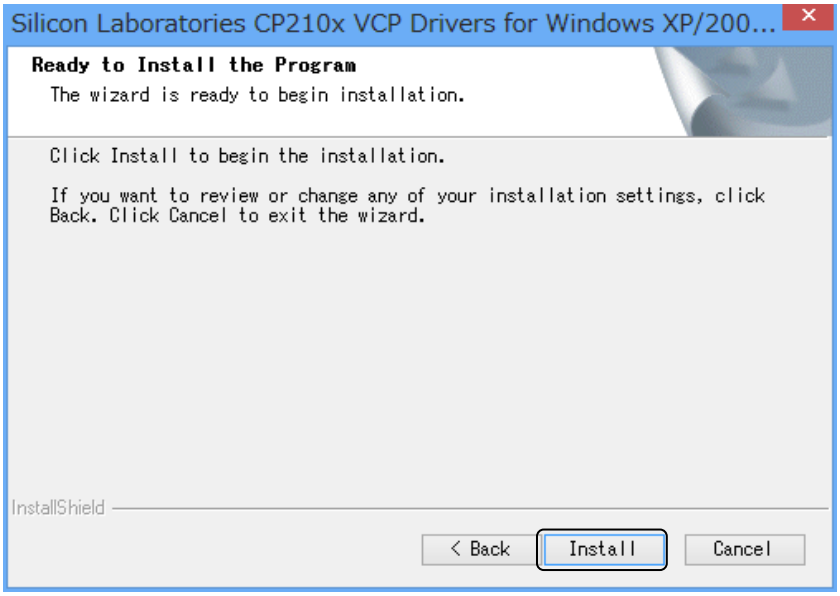

Silicon Laboratories CP210x VCP Drivers for Windows XP/200...
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

図2.4-6　Ready to Install the Program

手順5　〔Setup Status〕画面が表示され、インストールを開始します。その後、〔InstallShield Wizard Complete〕画面が表示されるので、〔Finish〕をクリックします。

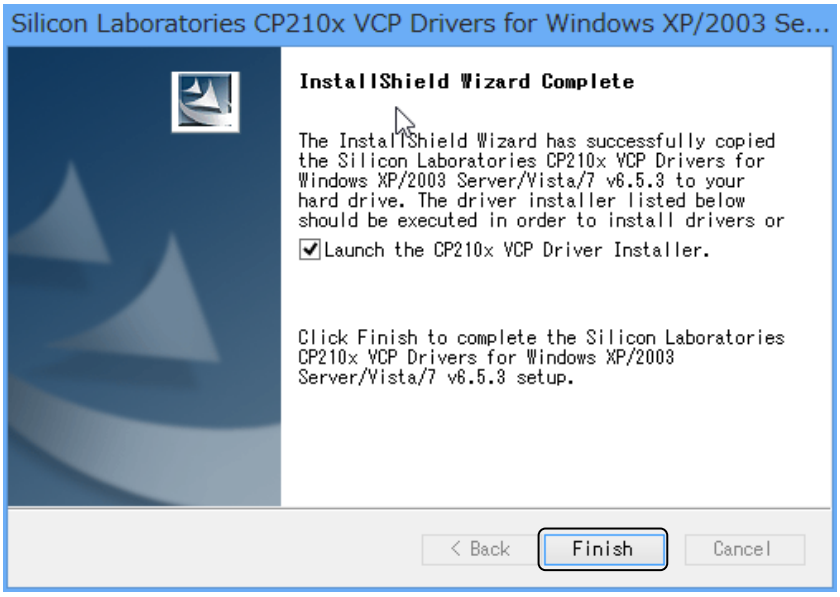

Silicon Laboratories CP210x VCP Drivers for Windows XP/2003 Se...
InstallShield Wizard Complete
The InstallShield Wizard has successfully copied the Silicon Laboratories CP210x VCP Drivers for Windows XP/2003 Server/Vista/7 v6.5.3 to your hard drive. The driver installer listed below should be executed in order to install drivers or
Launch the CP210x VCP Driver Installer.
Click Finish to complete the Silicon Laboratories CP210x VCP Drivers for Windows XP/2003 Server/Vista/7 v6.5.3 setup.
< Back
Finish
Cancel

図2.4-7　InstallShield Wizard Complete

手順6　〔Silicon Laboratories〕画面が表示されるので、〔Install〕をクリックします。

図2.4-8　Silicon Laboratories

手順7　〔Success〕画面が表示されるので、〔OK〕をクリックします。

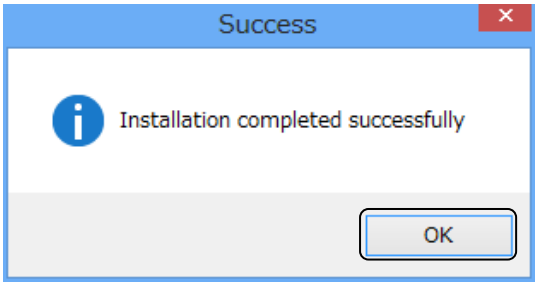


図2.4-9　Success

以上で USB ドライバのインストールは終了です。

◆シリアル接続コンソールの通信ソフト設定
コンソール用 PC 上の通信ソフトを起動して、シリアルポートの設定を以下のように設定してください。通信ソフトの例として、フリーウェアの「Tera Term」等があります。

表2.4-1　コンソールの通信ソフト設定

設定項目	内容
シリアルポート	コンセントレータと接続しているポート番号
通信速度（ボー・レート）	115200 bit/s
データ長	8 bit
パリティ	なし
ストップビット	1 bit
フロー制御	なし

CLI コンソールのログイン・ログアウト方法について説明します。
◆コンソール画面の表示
コンソール用 PC 上の通信ソフトを起動して、コンセントレータとシリアル接続または TCP/IP 接続を行ってください。
通信ソフトの画面が以下のように表示されたら、接続は完了です。

```
Login   :
        ↑   ユーザ名入力待ちになります。
```

◆ユーザ種別
ユーザ名、パスワードについては、「2.2 ユーザ名とパスワードの変更」を参照してください。

◆ログイン
ユーザ名とパスワードを入力してください。ユーザ名とパスワードが正しい場合、該当するユーザレベルのプロンプトが表示され、コンソールの操作が可能となります。

```
Login       : root
Password    : *****
                ↑   管理ユーザのユーザ名、パスワードを入力します。（例）
#
↑   管理ユーザのプロンプトを表示します。
```

◆ログアウト
ログアウトコマンドを入力してください。ログアウトコマンドを入力後、通信ソフトが終了します。
コンセントレータの不正操作を防ぐために、操作をしないときは必ずログアウトをしてください。

```
# exit
  ↑   ログアウトコマンドを入力します。
```

第３章　装置の基本設定

コンセントレータの基本的な設定を行うための手順について、説明します。

3.1　基本設定の流れ

コンセントレータの基本的な設定は、以下の手順で行います。

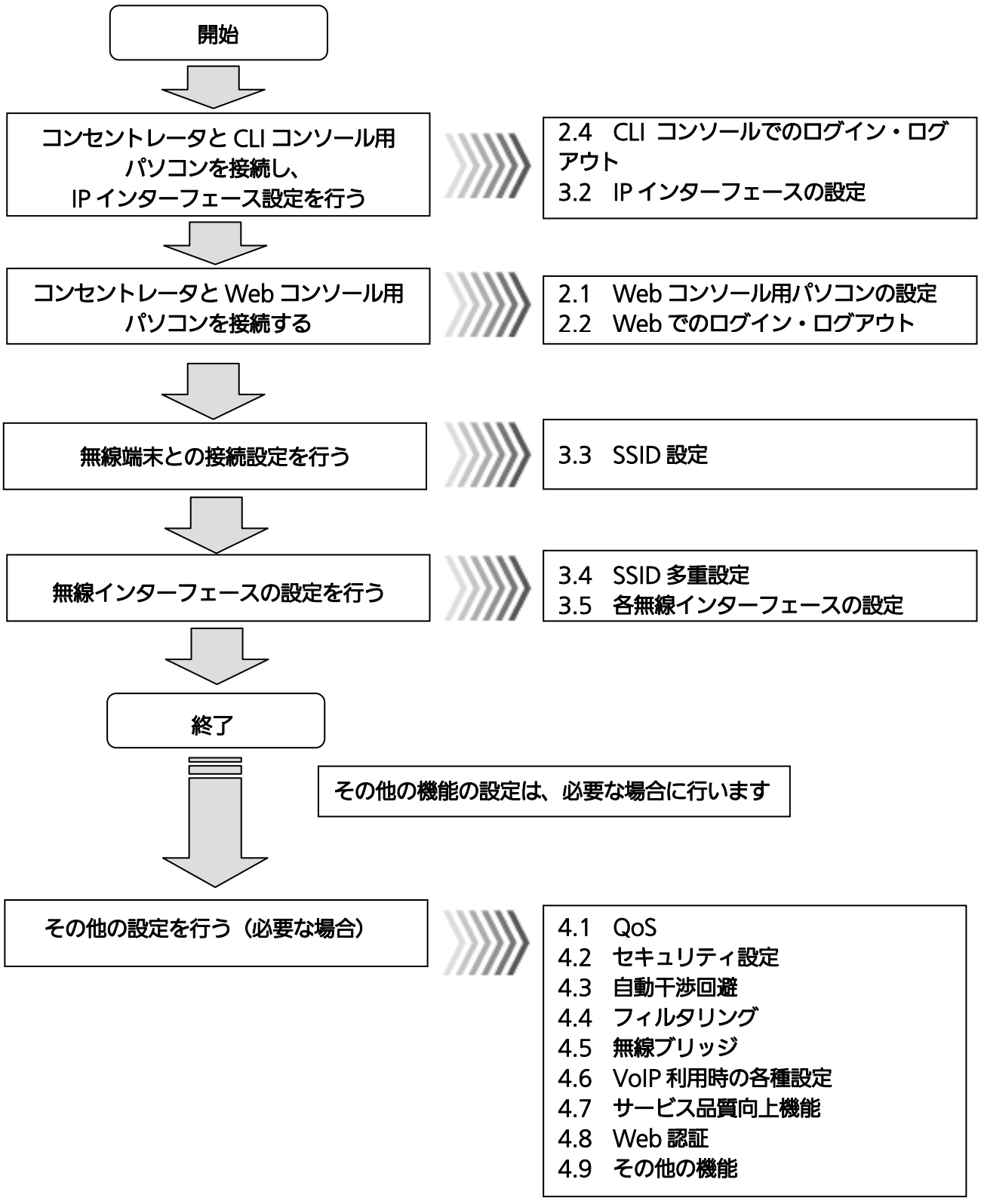


図3.1-1　ネットワーク構成手順

ここでは、下図の「営業部門用ネットワーク」へ接続する場合の設定を紹介します。

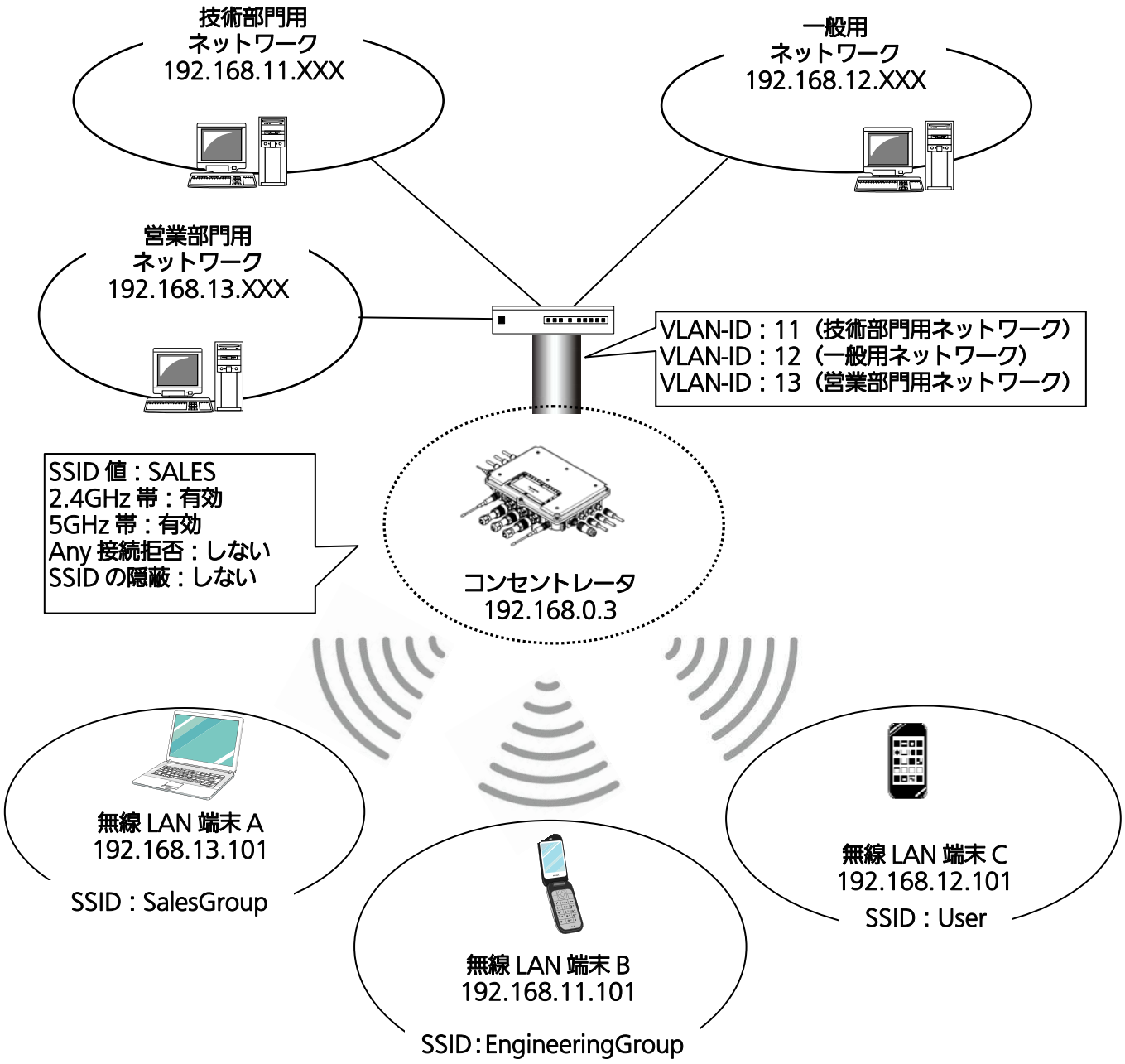


図3.1-2　ネットワーク構成例

Web コンソールを使用したコンセントレータの各設定値の確定、設定データの保存、リセット（自装置の再起動）について説明します。

操作手順

◆設定値の確定

各設定画面で行った設定を確定させるために、必ず各設定画面左下の〔設定〕をクリックしてください。

手順1　各設定画面左下の〔設定〕をクリックし、設定を確定します。

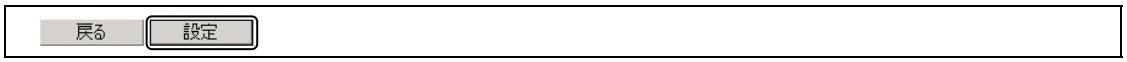


図3.1-3　設定ボタン

・ クリック後にエラーポップアップが出た場合は、設定漏れなどの可能性があるので、画面右上の〔更新〕をクリックし、最新の設定状態を画面で確認してください。

図3.1-4　設定の更新

◆設定データの保存

設定が完了したら、最後に必ず設定データを保存します。

手順1　画面右上の〔保存〕をクリックし、設定した内容をコンセントレータに保存します。

図3.1-5 設定の保存

重要	■ 設定データの保存処理中は、絶対に装置の電源を切らないでください。

◆リセット

自装置を再起動する手順を説明します。

手順1　〔システム系〕　→　〔保守〕　→　〔リセット〕を選択します。

図3.1-6　リセット

手順2　自装置再起動の〔実行〕をクリックします。

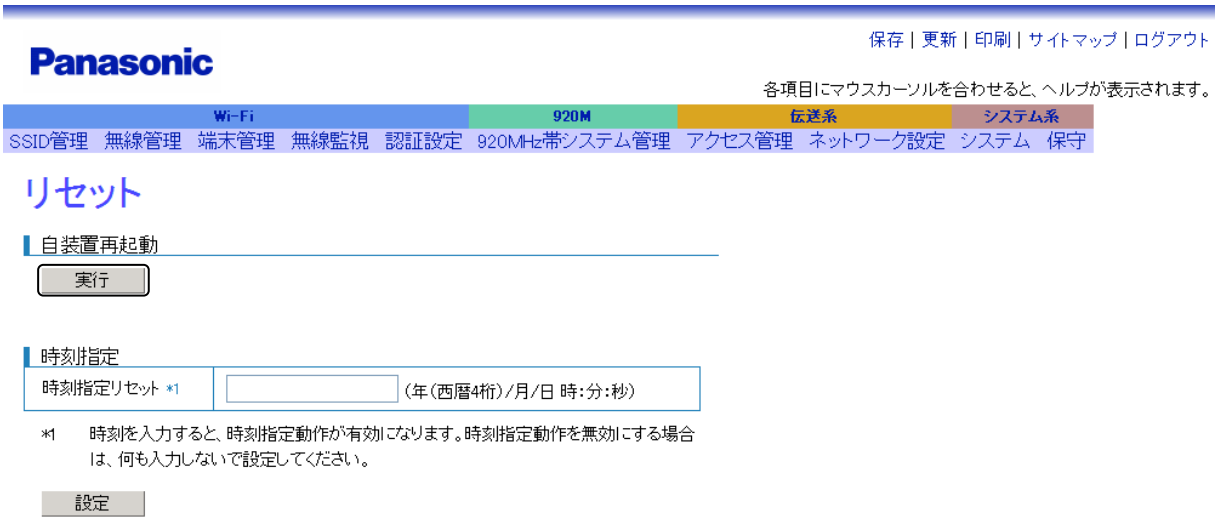


図3.1-7　自装置再起動

手順3　ポップアップ画面の〔ＯＫ〕をクリックすると、装置が再起動します。

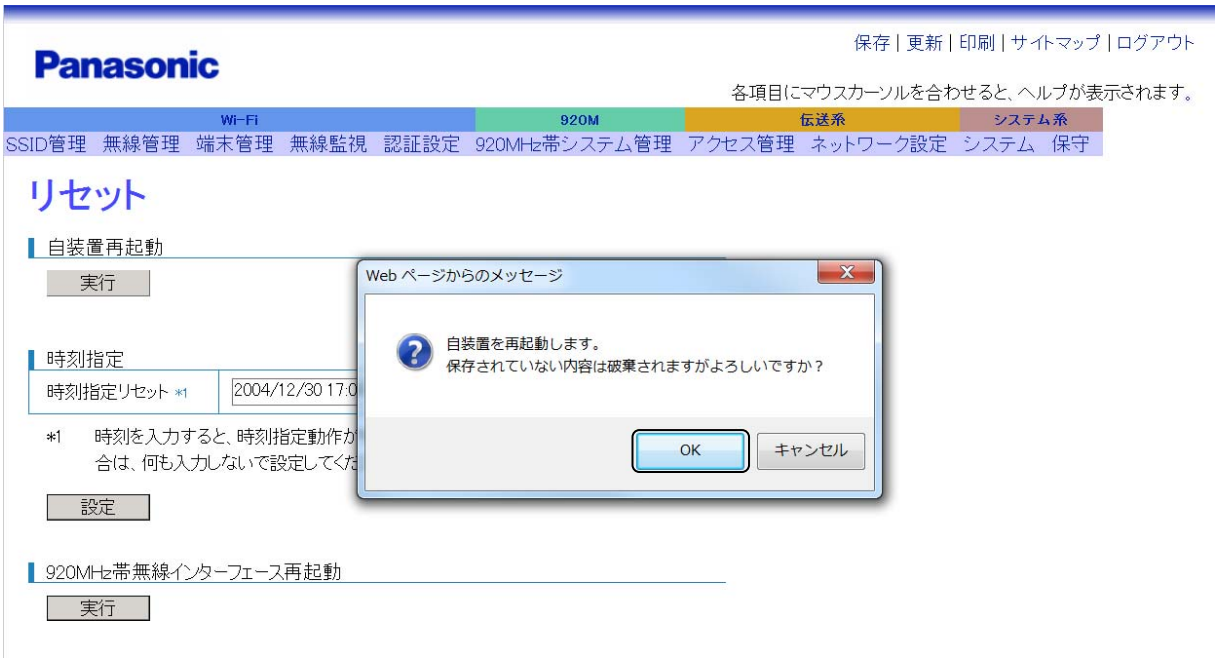


図3.1-8　ポップアップ画面

＜リセット後の各インターフェースの設定値＞

インターフェース	設定値	備考
WiFi インターフェース＃1（R11,R12,R13）	直前に保存されている設定値が有効になります。	
WiFi インターフェース＃2（R21,R22,R23）	直前に保存されている設定値が有効になります。	
920 MHz インターフェース（R31,R32）	直前に保存されている設定値が有効になります。	
イーサネット（E1,E2,E3）	直前に保存されている設定値が有効になります。	

3.2　IP インターフェースの設定

ここでは、ネットワークにコンセントレータを接続するための基本的な設定方法を説明します。

コンセントレータはマルチプル IP 対応により、IP アドレスを 16 個まで設定することが可能で、それぞれ独立した管理系ネットワークに所属させ監視・保守を行うことができます。各 IP インターフェースに設定する IP アドレスは、固定的設定に加えて DHCP プロトコルを使用することにより、DHCP サーバから IP アドレスを取得することができます。
また、各 IP インターフェースが所属する管理系ネットワークの VLAN 設定も行うことができます。

設定手順

◆IP アドレスの設定

例として、IP インターフェース 1 番に対して設定を行います。IP アドレス設定には CLI コンソールを使用します。

手順1　管理ユーザでログインします。

```
Login        : root
Password     : *****

#
```

手順2　IP インターフェース 1 番を有効にします。

```
# admin ip status 1 enabled

#
```

手順3　IP インターフェース 1 番の動作モードを〔static〕にします。

```
# admin ip mode 1 static

#
```

動作モードは以下の通りとなります。

static	: IP アドレス固定（static）動作
dhcp	: IP アドレス取得（DHCP）動作
ppp	: IP アドレス取得（PPP）動作

動作モード設定が「dhcp」で DHCP サーバと通信ができなかった場合、「static」設定の設定値が反映されます。（IP インターフェース 1 番はあらかじめ、初期値：192.168.0.3 が入力されていますので、DHCP サーバと通信ができなかった場合は、IP アドレス＝192.168.0.3 で運用します）

手順4　IP インターフェース 1 番に対して IP アドレスを設定します。

例として、下記内容での設定を示します。

- IP アドレスに「192.168.0.3」を入力
- サブネットマスクに「255.255.255.0」を入力
- デフォルトゲートウェイに「192.168.0.1」を入力

```
# admin ip set 1 192.168.0.3 255.255.255.0 192.168.0.1

#
```

設定手順

◆VLAN（Admin VLAN）の設定

例として､IP インターフェース 1 番に対して設定を行います｡VLAN 設定には CLI コンソールを使用します。

手順1　IP インターフェース 1 番に対して VLAN-ID、CoS 値を設定します。

例として、下記内容での設定を示します。

- VLAN-ID：｢11｣、CoS 値：｢7｣を入力

```
# admin vlan vlanid 1 vlanid 11

# admin vlan cos 1 7

#
```

手順2　IP インターフェース 1 番に対して VLAN モードを設定します。

例として、下記内容での設定を示します。

- VLAN モード：〔シングルタグ〕を選択

```
# admin vlan mode 1 singletag

#
```

重要

- ■ IP インターフェース設定変更完了後は、Web コンソール用パソコン側のネットワーク、VLAN 設定を無線 LAN アクセスポイントの設定に合わせて変更してください。設定した値によっては、以降の接続ができなくなりますのでご注意ください。
- ■ 同時に設定可能な PPP 接続は 1 つです。
- ■ IP の変更を行った場合、Web ログイン、Telnet ログインは自動でログアウトされます。

3.3　SSID の設定

コンセントレータに異なる複数の SSID を設定し、各 SSID に異なる VLAN をマッピングさせることで、1 つのシステムで独立した複数のネットワーク接続を提供することができます。
SSID は最大 16 個までコンセントレータに多重できますので、仮想 AP が 16 台まで設定されることになります。コンセントレータはデュアルバンド（2.4GHz／5GHz）の無線インターフェースを搭載しており、同じ SSID が仮想 AP の
各無線インターフェースに設定されますので、ユーザは無線 LAN 端末のインターフェースを意識することなく、コンセントレータと接続し通信を行うことができます。

設定手順

◆SSID の生成

ここからは、Web コンソールを使用して設定します。

手順1　〔Wi-Fi〕　→　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

図3.4-1　メニュー（SSID 設定）

手順2　〔SSID 生成〕をクリックします。

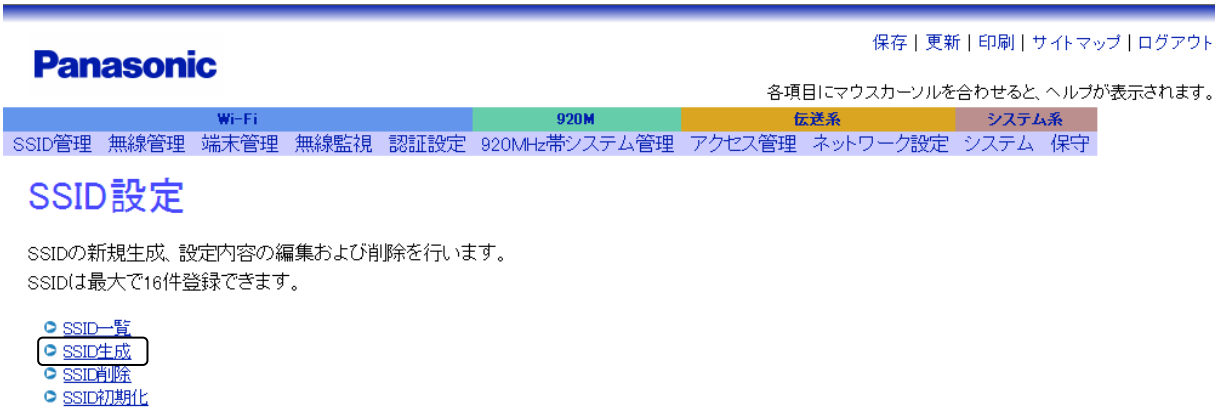


図3.4-2　SSID 設定

手順3　新たに作成する SSID のプロファイル名（SSID 名）を指定します。

例として、SSID 番号 1 に営業部門用の SSID 名「SalesGroup」を生成します。

・ SSID 番号〔1〕を選択

・ SSID 名に「SalesGroup」を入力

上記操作後、〔生成〕をクリックします。

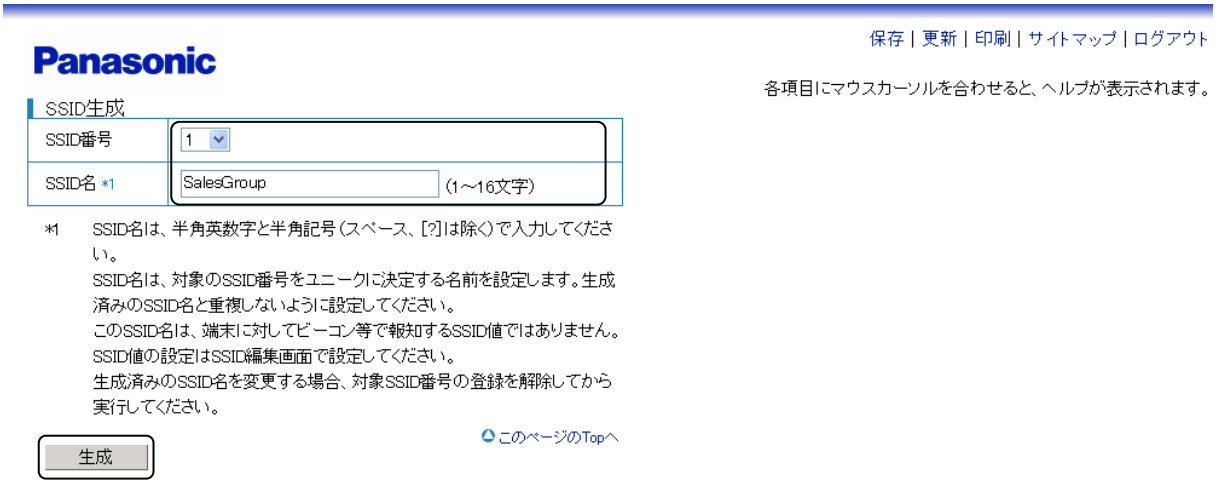


図3.4-3　SSID 生成

重要	■ ここで設定する SSID 名は、システム内で SSID を識別するために使用します。他の SSID の SSID 名と重複しないように設定してください。また、ビーコンに付与される SSID 値は、SSID 編集（後述）で使用します。

設定手順

◆SSID の設定

手順1　〔Wi-Fi〕 → 〔SSID 管理〕 → 〔SSID 設定〕を選択します。

図3.4-4　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

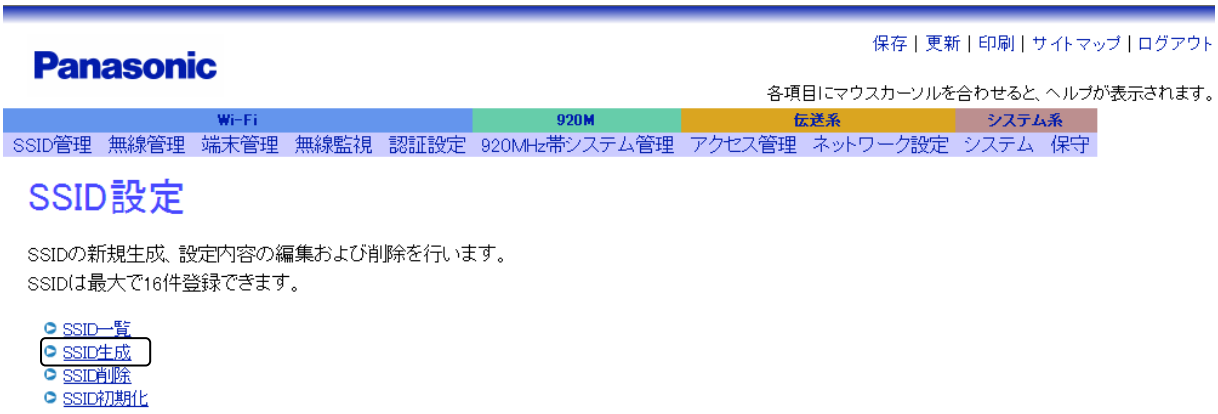


図3.4-5　SSID 設定

手順3　対象となる SSID の〔編集〕をクリックします。

例として、「SalesGroup」の編集を行います。

図3.4-6　SSID 一覧

〔SSID 編集〕画面が表示されます（図 3.4-7）。こちらより SSID の各種設定を行います。

図3.4-7　SSID 編集

手順4　〔SSID 情報〕をクリックし、SSID 値を設定します。

例として、SSID 名「SalesGroup」に対して SSID 値「SALES」を設定します。
ここで設定した SSID 値が ビーコン に付与されます。

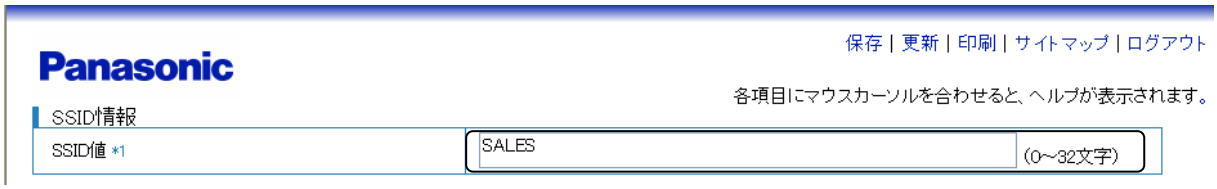


図3.4-8　SSID 情報

手順5　〔SSID 編集〕画面（図 3.4-7）の〔利用する無線インターフェース〕をクリックし、利用する無線インターフェースを〔有効〕にします。

例として、IF1、IF2 の両方を有効にします。

図3.4-9　利用する無線インターフェース

手順6　〔SSID 編集〕画面（図 3.4-7）の〔無線モード〕をクリックし、2.4GHz 帯と 5GHz 帯の無線モードを選択します。

例として、下記内容での設定を示します。

- 11bgn モード：〔11bgn〕を選択
- 11an モード：〔11an〕を選択

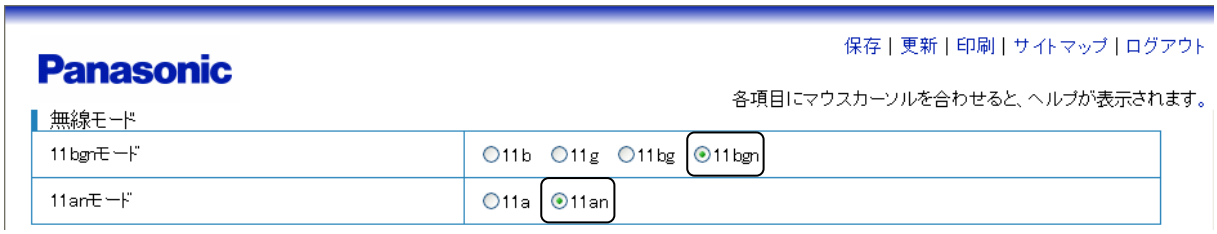


図3.4-10　無線モード

手順7　〔SSID 編集〕画面（図 3.4-7）の〔IEEE802.11 設定〕をクリックし、IEEE802.11 に 関する設定を行います。

802.11 認証アルゴリズムに関して、詳細は「4.2　セキュリティ設定」をご参照ください。

例として、下記内容での設定を示します。

- Any 接続拒否：〔しない〕を選択（無線 LAN 端末からコンセントレータを検索可とします。）
- SSID の隠蔽：〔しない〕を選択（ビーコンに SSID 名を載せます。）

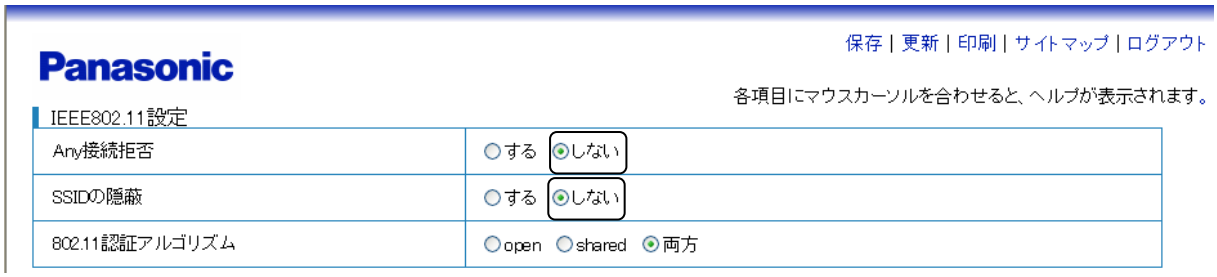


図3.4-11　IEEE802.11 設定

手順8　〔SSID 編集〕画面（図 3.4-7）の〔VLAN モード〕をクリックし、VLAN モードを選択します。

〔SSID〕を選択した場合は、SSID ごとに VLAN を分離します。

〔SSID ＆ User〕、〔User〕については、「4.2.4 ユーザ認証」をご参照ください。

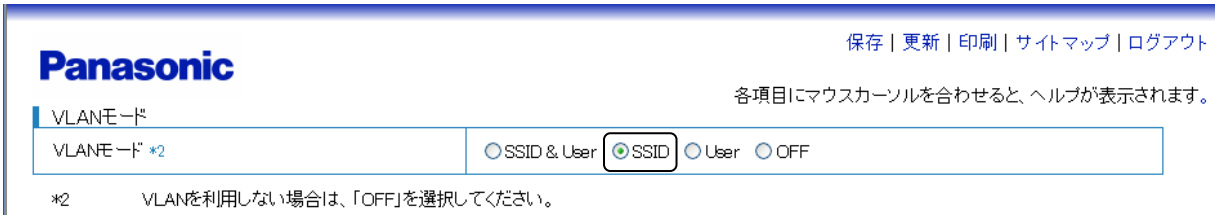


図3.4-12　VLAN モード

手順9　〔SSID 編集〕画面（図 3.4-7）の〔SSID VLAN〕をクリックし、VLAN-ID を設定します。

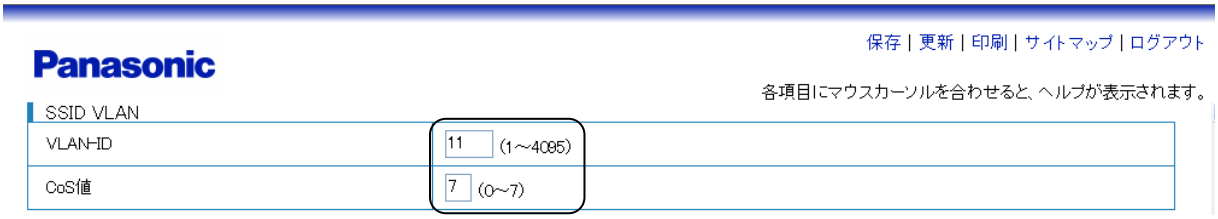


図3.4-13　SSID VLAN

手順 8 にて「User」、または「SSID & User」を選択した場合は、〔User VLAN〕の設定を行います。（図 3.4-14）

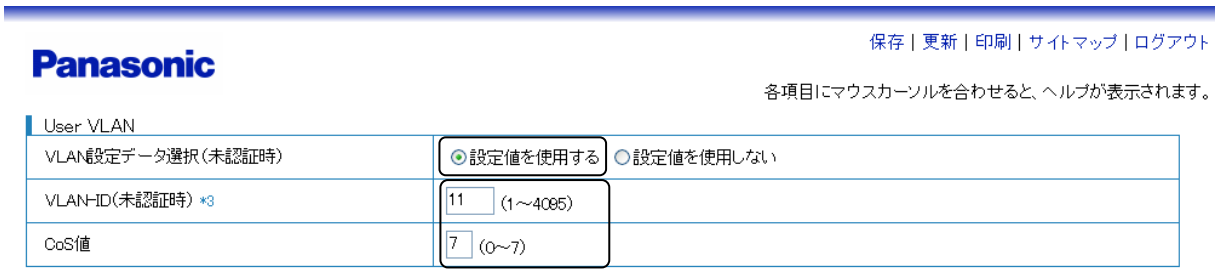


図3.4-14　User VLAN

手順10　画面最下部の〔設定〕を押し、設定を反映させます。

■以下の編集項目については、各種機能設定を参照ください。

・セキュリティ(EAP 認証) ・IEEE802.1X 認証 ・暗号鍵更新設定 ・MAC 認証 ・認証動作設定 ・Authentication・Accounting ・無線プロビジョニングサービス ・連続接続制限	4.2　セキュリティ設定
・代理 ARP 応答 ・通信端末数による端末接続制御	4.6　VoIP 利用時の各種設定
・QoS	4.1　QoS
・IGMP スヌーピング	4.7　サービス品質向上機能
・Web 認証 ・Web 認証 AP 間連携	4.8　Web 認証
・アグリゲーション ・LDPC 符号化	4.9　その他の機能

3.4　SSID 多重設定

無線インターフェース（IF1）と無線インターフェース（IF2）における、SSID ごとの送信制御やデータレートの設定を行います。

設定手順

◆SSID 多重での SSID 動作設定

SSID の生成と設定は前節にて実施済みとします。

手順1　〔Wi-Fi〕 → 〔無線管理〕 → 〔SSID 多重設定〕を選択します。

図3.5-1　メニュー（SSID 多重設定）

手順2　対象となる SSID の〔編集〕をクリックします。

例として、登録番号：1 の編集を行います。

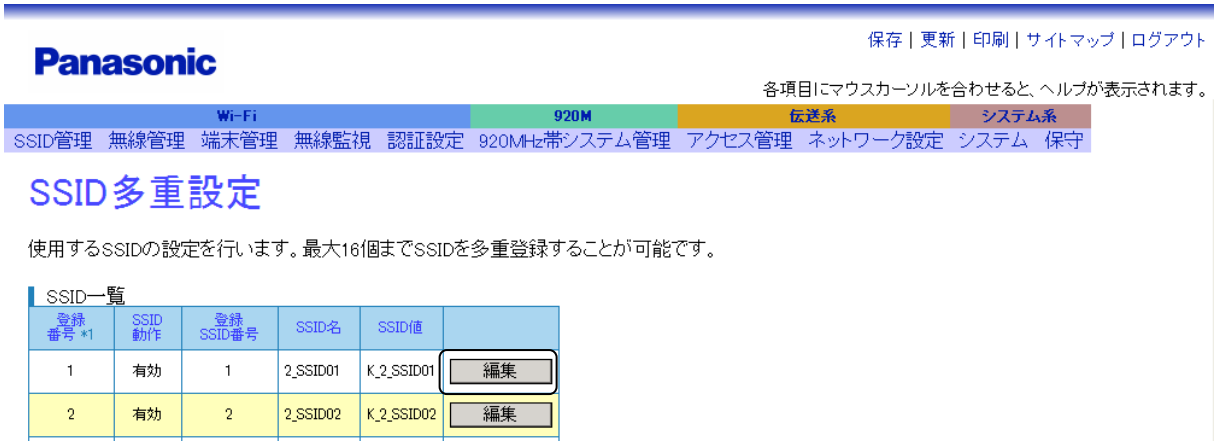


図3.5-2　SSID 多重設定

手順3　〔SSID 登録〕をクリックします。

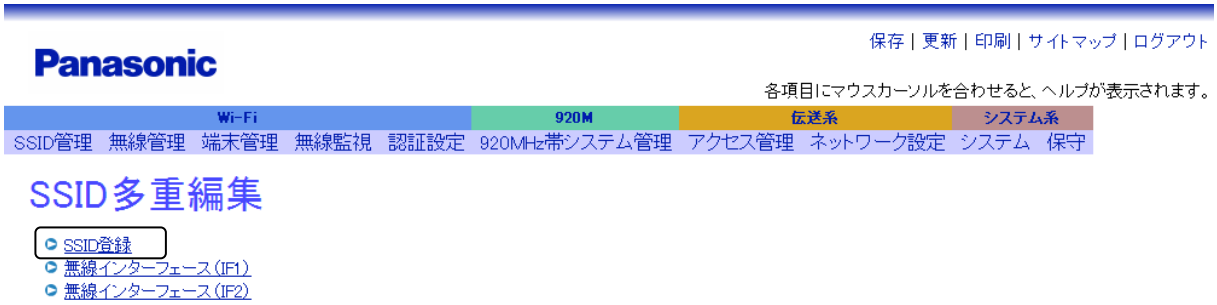


図3.5-3　SSID 多重編集

手順4　SSID 登録を行います。

例として、下記内容での設定を示します。

- SSID 動作：〔有効〕を選択
- 登録 SSID 番号：〔1〕を選択（手順 2 で選択した登録番号に紐付けする SSID 番号を選択。）

図3.5-4　SSID 登録

手順5　〔SSID 多重編集〕画面（図 3.5-3）の〔無線インターフェース（IF1）〕、または〔無線インターフェース（IF2）〕をクリックし、マルチキャスト・ブロードキャストの送信制御、および各種データレート設定を行います。

例として、無線インターフェース（IF1）に以下の設定をした場合の設定画面を示します。

- ブロードキャスト制御：〔送信遮断を行わない〕を選択
- マルチキャスト制御：　〔送信遮断を行わない〕を選択
- 制御モード：〔自動〕を選択
- 最小値（レガシー）：〔1M〕を選択
- 最大値（レガシー）：〔54M〕を選択
- 最小値（11n）：〔15M〕を選択
- 最大値（11n）：〔450M〕を選択
- ブロードキャストレート制御：〔無効〕を選択
- マルチキャストレート制御：〔無効〕を選択
- ビーコンレート制御：〔無効〕を選択

図3.5-5　2.4GHz 帯設定（SSID 多重設定）

〔無線インターフェース（IF2）〕も 〔無線インターフェース（IF1）〕の画面（図 3.5-5）と同様です。

データシート(レガシー)の大きさは、
11b（1M＜2M＜5.5M＜11M）＜11g（6M＜9M＜12M＜18M＜24M＜36M＜48M＜54M）の順になります。
また、ブロードキャスト／マルチキャスト／ビーコンのレート設定を使用する場合は、それぞれのレート制御モードを「有効」に設定してください。

帯域比率について、詳細は「4.1　QoS」をご参照ください。
11n レートの設定は、周波数帯域幅 40MHz、GI=400ns を基準に行います。
実際に設定する送信レートは、選択するレート制御項目によって変わりますので、下表を参照のうえ、設定レート列の値を設定してください。

例）周波数帯域幅：20MHz、最高送信レート：450M を指定した場合は、最高送信レートとして 216.7M を設定します。（GI：400ns の場合）

表3.5-1　レート制御

MCS *	変調方式	符号化率	空間多重数	データレート				設定レート
				20MHz		40MHz		
				GI=800ns	GI=400ns	GI=800ns	GI=400ns	
0	BPSK	1/2	1	6.5	7.2	13.5	15.0	15.0
1	QPSK	1/2	1	13.0	14.4	27.0	30.0	30.0
2	QPSK	3/4	1	19.5	21.7	40.5	45.0	45.0
3	16QAM	1/2	1	26.0	28.9	54.0	60.0	60.0
4	16QAM	3/4	1	39.0	43.3	81.0	90.0	90.0
5	64QAM	2/3	1	52.0	57.8	108.0	120.0	120.0
6	64QAM	3/4	1	58.5	65.0	121.5	135.0	135.0
7	64QAM	5/6	1	65.0	72.2	135.0	150.0	150.0
8	BPSK	1/2	2	13.0	14.4	27.0	30.0	30.0
9	QPSK	1/2	2	26.0	28.9	54.0	60.0	60.0
10	QPSK	3/4	2	39.0	43.3	81.0	90.0	90.0
11	16QAM	1/2	2	52.0	57.8	108.0	120.0	120.0
12	16QAM	3/4	2	78.0	86.7	162.0	180.0	180.0
13	64QAM	2/3	2	104.0	115.6	216.0	240.0	240.0
14	64QAM	3/4	2	117.0	130.0	243.0	270.0	270.0
15	64QAM	5/6	2	130.0	144.4	270.0	300.0	300.0
16	BPSK	1/2	3	19.5	21.7	40.5	45.0	45.0
17	QPSK	1/2	3	39.0	43.3	81.0	90.0	90.0
18	QPSK	3/4	3	58.5	65.0	121.5	135.0	135.0
19	16QAM	1/2	3	78.0	86.7	162.0	180.0	180.0
20	16QAM	3/4	3	117.0	130.0	243.0	270.0	270.0
21	64QAM	2/3	3	156.0	173.3	324.0	360.0	360.0
22	64QAM	3/4	3	175.5	195.0	364.0	405.0	405.0
23	64QAM	5/6	3	195.0	216.7	405.0	450.0	450.0

＊MCS：Modulation and Coding Scheme

手順6　画面最下部の〔設定〕を押し、設定を反映させます。

3.5　SSID 設定情報コピー

無線インターフェース（IF1）と無線インターフェース（IF2）における、SSID 設定情報をコピーします。

設定手順

◆無線インターフェースの設定

手順1　〔SSID 管理〕　→　〔SSID 設定情報コピー〕を選択します。

図3.5-6　メニュー（SSID 設定情報コピー）

手順2　〔SSID 管理〕　→　〔SSID 設定情報コピー〕を選択します。

例として、SSID 番号 1 の内容を SSID 番号 2 にコピーをするとします。

- コピー元 SSID 番号で SSID 番号〔1〕を選択
- コピー先 SSID 番号で SSID 番号〔2〕を選択

上記操作後、〔コピー〕をクリックします。

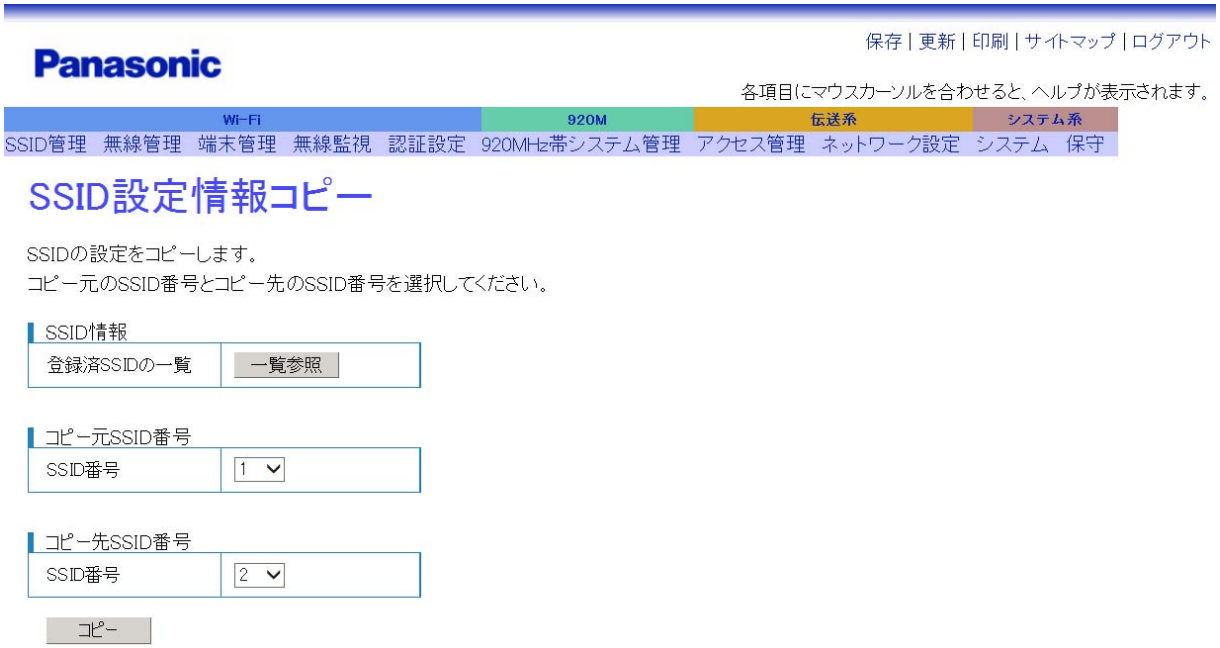


図3.5-7　SSID 設定情報コピー

3.6　各無線インターフェースの設定

2.4GHz 帯・5GHz 帯それぞれの周波数帯における、詳細設定を行います。

設定手順

◆無線インターフェースの設定

手順1　〔Wi-Fi〕　→　〔無線管理〕　→　〔インターフェース（IF1）設定〕、または〔インターフェース（IF2）設定〕を選択します。

例として、インターフェース（IF1）　設定を選択します。

図3.6-1　　メニュー（無線管理）

手順 2 ～ 手順 4 は〔インターフェース(IF1)設定〕画面（図 3.6-2）より各種設定を行います。

図3.6-2　　インターフェース(IF1)設定

手順2　〔インターフェース(IF1)設定〕画面（図 3.6-4）で〔周波数帯域変更設定〕をクリックします。

例として、下記内容での設定を示します。

・ 周波数帯域（次回起動時有効値）：〔4.9GHz〕を選択

・ 上記操作後、〔切替〕をクリックします。

※周波数帯域の設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

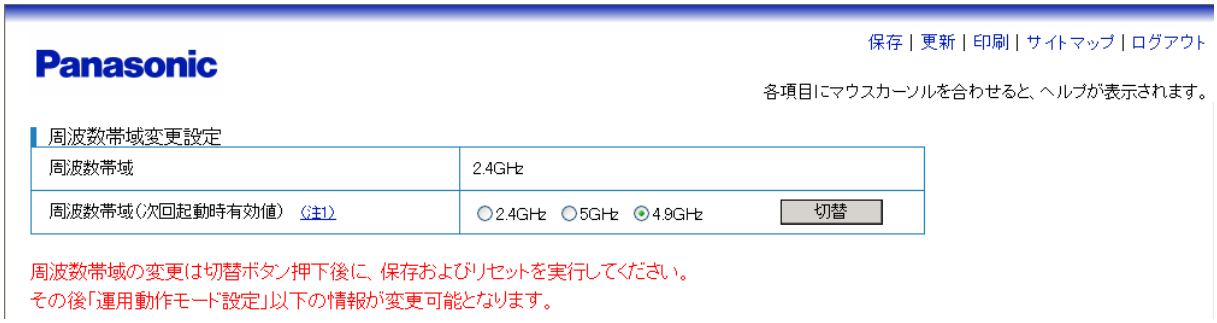


図3.6-3　運用動作モード設定

手順3　〔インターフェース（IF1）設定〕画面（図 3.6-4）で〔運用動作モード〕をクリックします。

例として、下記内容での設定を示します。

・ 無線インターフェース：〔有効〕を選択

・ 動作モード：〔通常運用〕を選択

図3.6-4　運用動作モード設定

4.9GHz 帯無線ブリッジを使用する場合、長距離伝送無線送信モードを〔遅延送信〕に設定し、長距離伝送無線通信距離を実際の距離に合わせて設定してください。

手順4　〔インターフェース(IF1)設定〕画面（図 3.6-2）で〔チャネル制御〕をクリックします。

例として、下記内容での設定を示します。

・ チャネル制御モード：〔自動〕を選択

図3.6-5　チャネル制御（4.9GHz）

手順5　画面最下部の〔設定〕をクリックし、設定を反映させます。

5GHz 帯設定時は、図 3.6-6　の画面が表示されます。

図3.6-6　チャネル制御（5GHz）

重要	■ 5GHz 帯でのみ 40MHz 運用が可能なため、2.4GHz 設定では周波数帯域幅は 20MHz、40MHz 復旧監視機能は無効のみ設定可能です。

その他、周波数帯における詳細設定の変更を行う場合は、以降の設定を行います。

◆接続端末制御

対象無線インターフェースの最大接続可能端末数を設定します。

※この設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

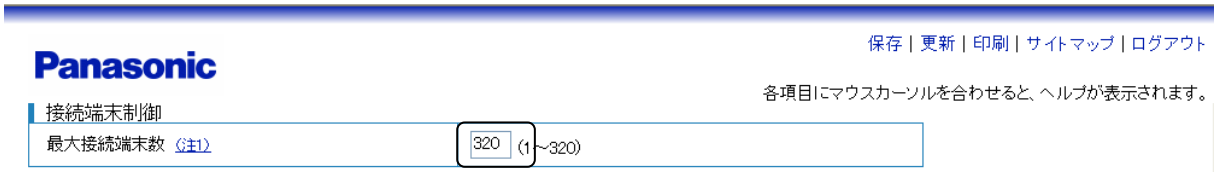


図3.6-7　接続端末制御

◆モニタ

全チャネルスキャンの有効／無効を設定します。

有効を選択した場合は、モニタ間隔を設定します。

※モニタ：〔有効〕を設定した場合、パケットロスが発生したり、接続した端末が切断される可能性があります。

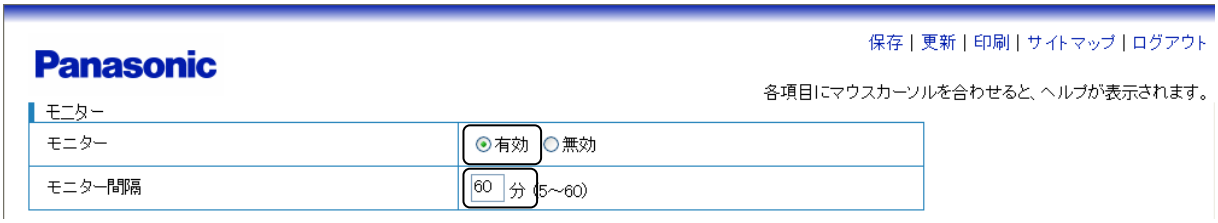


図3.6-8　モニタ

◆干渉回避

チャネル制御を自動で行っている際、干渉により使用可能なチャネルが存在しなかった場合の最終動作を選択します。

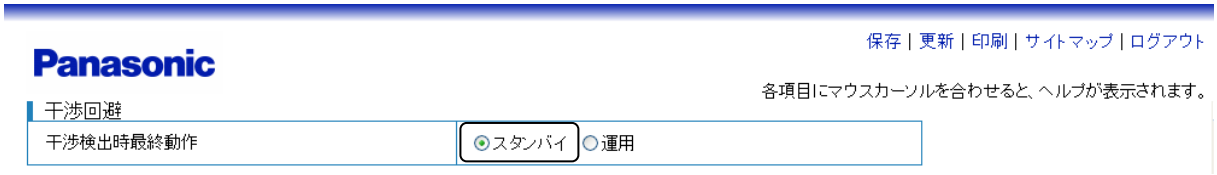


図3.6-9　干渉回避

◆無線ブリッジ

無線ブリッジにおける各設定を行います。（詳細は、4.5 無線ブリッジを参照してください。）

※〔無線ブリッジ動作許可設定〕の変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

図3.6-10　無線ブリッジ

◆帯域制御

コンセントレータと無線 LAN 端末間でのパケットの帯域制御方法を設定します。

※この設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。なお、本機能の詳細は「4.1　QoS」をご参照ください。

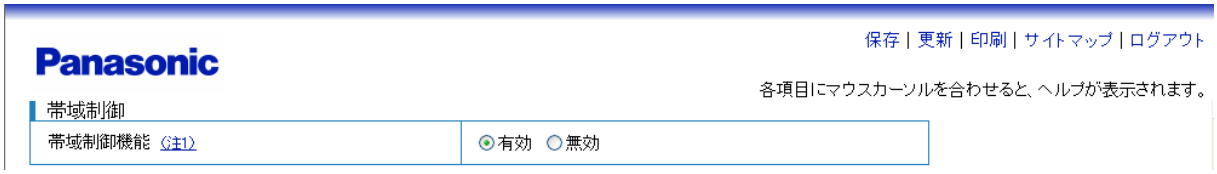


図3.6-11　帯域制御

◆受信電波強度による端末接続制御

接続している端末台数が設定した閾値に達した場合、電波の弱い端末の接続要求を拒否する機能の設定を行います。

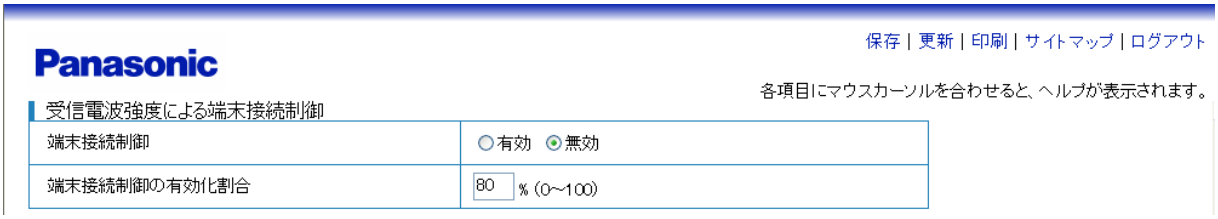


図3.6-12　受信電波強度による端末接続制御

◆プロテクション

11n 未対応端末に対する干渉保護動作（HT プロテクション動作）の設定を行います。

図3.6-13　プロテクション

第４章　各種機能設定

コンセントレータの各種機能について、説明します。

4.1　QoS

コンセントレータの QoS 機能（優先制御・帯域制御）設定について説明します。

4.1.1　SSID ごとの帯域制限

帯域制御設定とは、コンセントレータが提供する QoS 機能の 1 つであり、マルチアクセス コンセントレータに多重している SSID ごとに 10 段階の比率を設定することで、下りデータのトラフィック輻輳時に当該 SSID が使用できる帯域幅に差をつけることができます。
ここでは、下り無線区間輻輳時に SSID1 と SSID2 のトラフィックが利用できる帯域を割り当てる方法を紹介します。
以下の例では、下り無線区間輻輳時には、SSID1：SSID2＝5：1 の帯域を割り当てます。
この帯域制御動作は、無線区間の輻輳時に機能し、輻輳していない状態では必要な帯域を使用することができ、空き帯域を有効に利用できます。同じ SSID を使用する端末の帯域比率は均等になります。

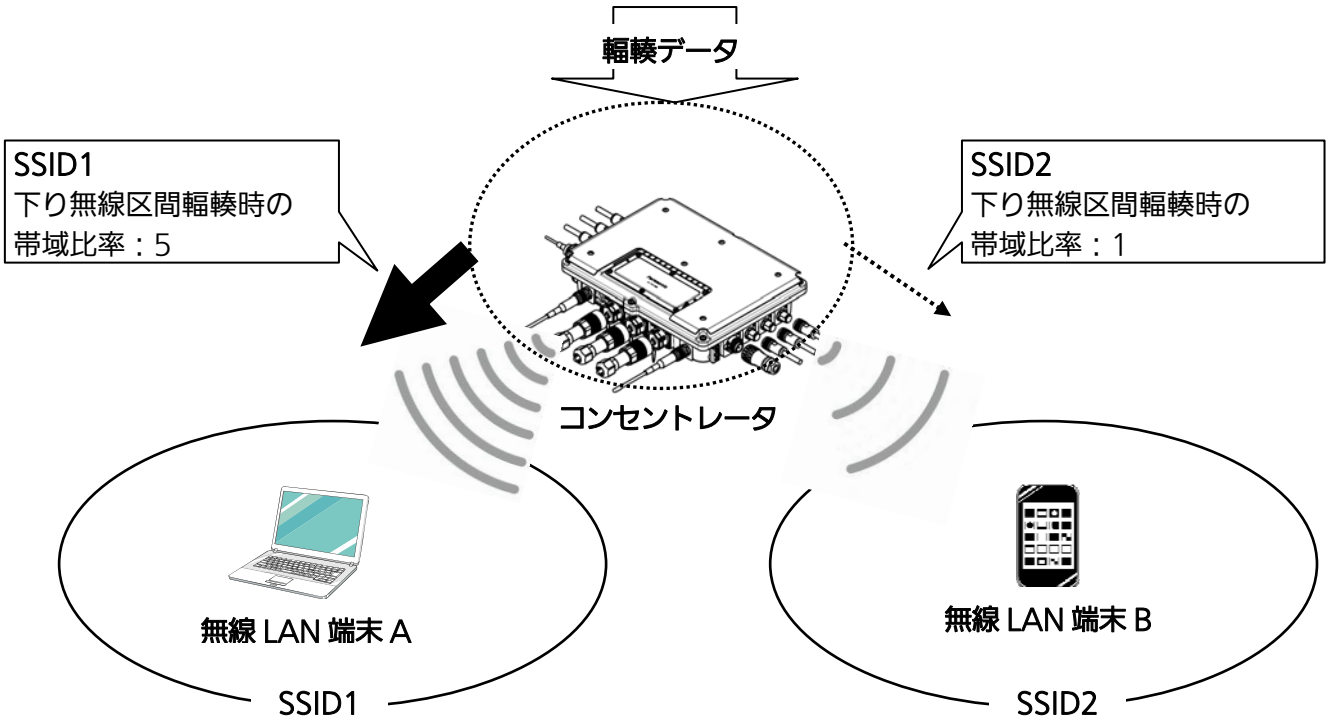


図4.1-1　帯域制御動作

設定手順

◆帯域制御の設定

ここではインターフェース(1F1)設定の設定を行うものとします。

手順1　〔Wi-Fi〕　→　〔無線管理〕　→　〔インターフェース(1F1)設定〕を選択します。

図4.1-2　メニュー（インターフェース(1F1)設定）

手順2　〔帯域制御〕をクリックします。

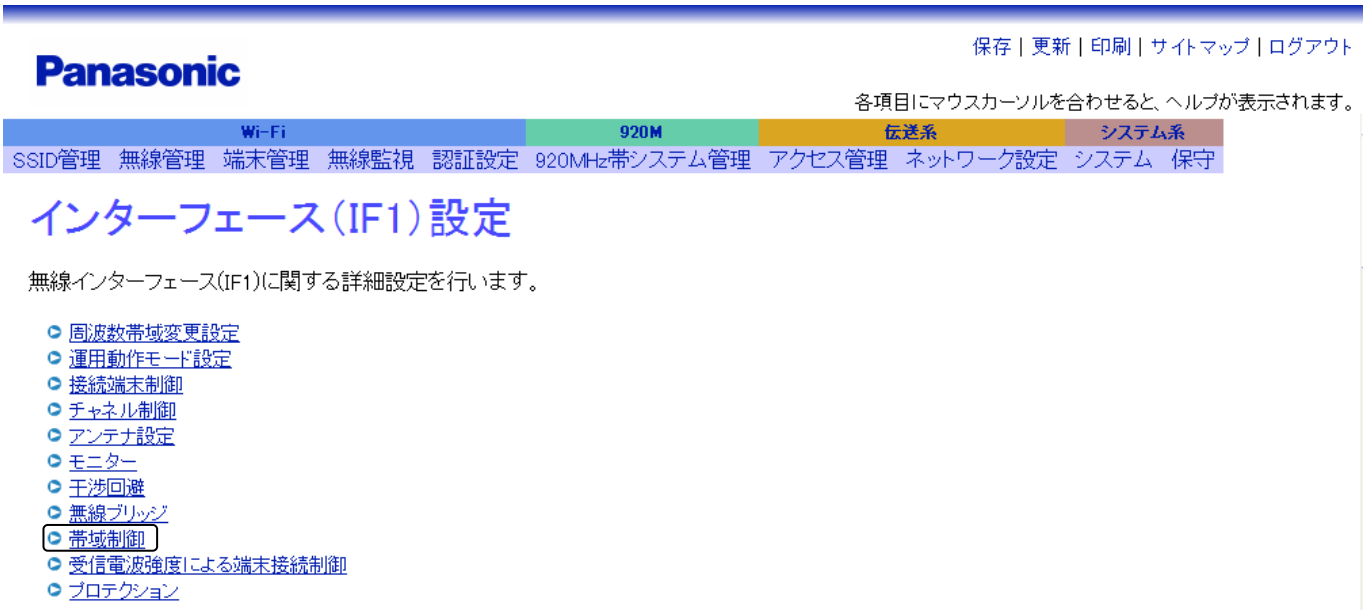


図4.1-3　インターフェース(1F1)設定

手順3　〔有効〕を選択します。

※この設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

図4.1-4　帯域制御

手順4　画面最下部〔設定〕をクリックし、設定を反映させます。

設定手順

◆帯域比率の設定

手順1　〔Wi-Fi〕　→　〔無線管理〕　→　〔SSID 多重設定〕を選択します。

図4.1-5　メニュー（SSID 多重設定）

手順2　対象となる SSID の〔編集〕をクリックしクリックします。

例として SSID1 を指定します。

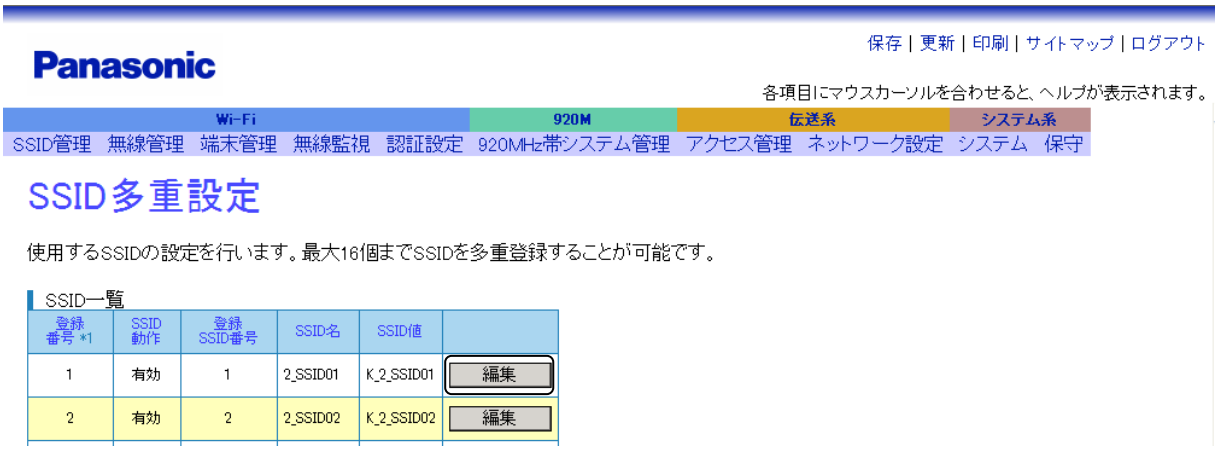


図4.1-6　SSID 多重設定

手順3　〔無線インターフェース（IF1)〕をクリックします。

図4.1-7　SSID 多重編集

手順4　「帯域比率」を（1～10）の任意の値で設定します。

例として「1」を入力します。

図4.1-8　無線インターフェース（IF1）設定（帯域比率）

手順5　画面最下部〔設定〕をクリックし、設定を反映させます。

※必要に応じて、同じ無線インターフェース番号に登録しているほかの SSID に対しても帯域を設定してください。

4.1.2　フローごとの優先制御

優先制御設定とは、コンセントレータが提供する QoS 機能の 1 つであり、SSID 内を流れるデータフレームの条件を定義し、その条件に一致するデータフレームを優先することができます。優先制御は、優先設定・CoS 値設定・ToS 値設定の 3 つの設定があり、無線 LAN 接続・無線ブリッジ接続それぞれに設定できます。条件には、ブリッジ条件、または IP 条件を用いることができます。

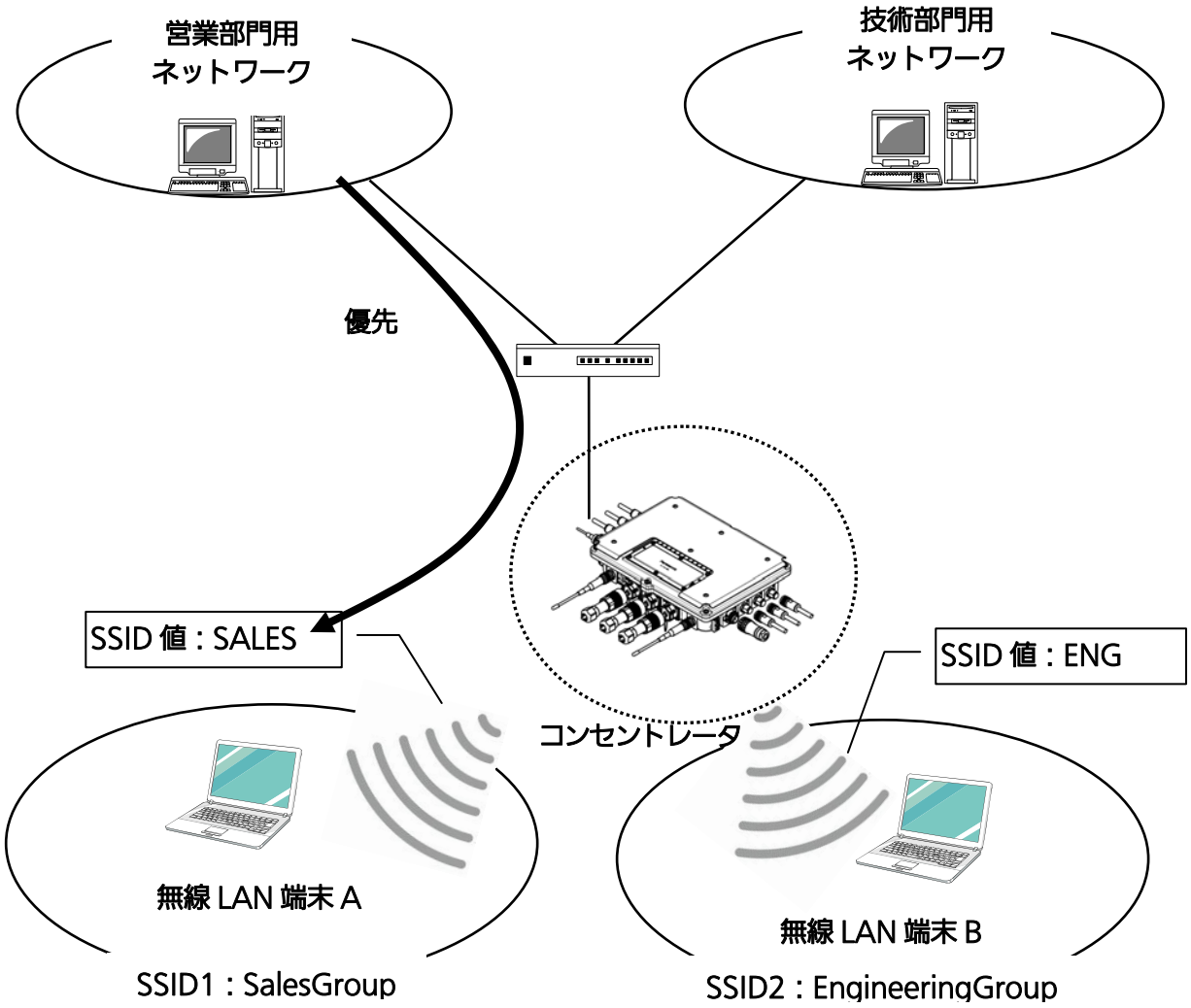


図4.1-9　優先制御例

■優先制御の動作モード

優先制御の動作モードには、WMM（WMM® （Wi-Fi Multimedia ™）に沿った QoS 制御）と WRR（重みつきラウンドロビン転送)、OFF（QoS 制御をしない）の 3 種類があります。WMM モードでは、WMM 対応無線 LAN 端末との間で上り下り方向無線データの優先制御を行うことができます。WRR モードでは、WMM 非対応無線 LAN 端末に対し、下り方向無線データの優先制御を行うことができます。

表4.1-1　動作モード一覧

モード	説明	備考
WMM	WMM 対応無線 LAN 端末と上り下り方向の無線データに対する優先制御を行います。	
WRR	下り方向の無線データに対する優先制御を行います。	・WPA/IEEE802.11i･WPA2 の認証モード時は設定できません。 ・SSID の無線モードが 11n 対応モード時は、WMM 固定で動作します。
OFF	QoS 制御を行わない。	・SSID の無線モードが 11n 対応モード時は、WMM 固定で動作します。

■優先制御の概要

WRR、WMM を選択した場合は、データフレームに優先制御の条件設定を行います。条件にはブリッジ条件と IP 条件があり、それぞれ送信元 MAC アドレスや送信先 MAC アドレス、送信元 IP アドレスや送信先 IP アドレスなどを条件として設定できます。ただし、WMM ではデータフレーム内の DSCP／CoS 値により自動的に下り方向無線データの優先度が割り当てられます。

表4.1-2　アクセスコントロールプライオリティの割当

設定項目	単位	値および意味	最大登録可能数
ブリッジ条件	装置	送信元 MAC アドレス 送信先 MAC アドレス イーサタイプ VLAN-ID CoS 値	512
IP 条件	装置	送信元 IP アドレス 送信元 IP マスク値 送信先 IP アドレス 送信先 IP マスク値 TOS 値 プロトコル番号 送信元ポート 送信先ポート	512
ブリッジ条件のプライオリティ	SSID	0～3：プライオリティ	32
IP 条件のプライオリティ	SSID	0～3：プライオリティ	32

条件設定の詳細は、「4.4　フィルタリング」を参照してください。

設定手順

◆優先制御の設定

手順1　〔Wi-Fi〕　→　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

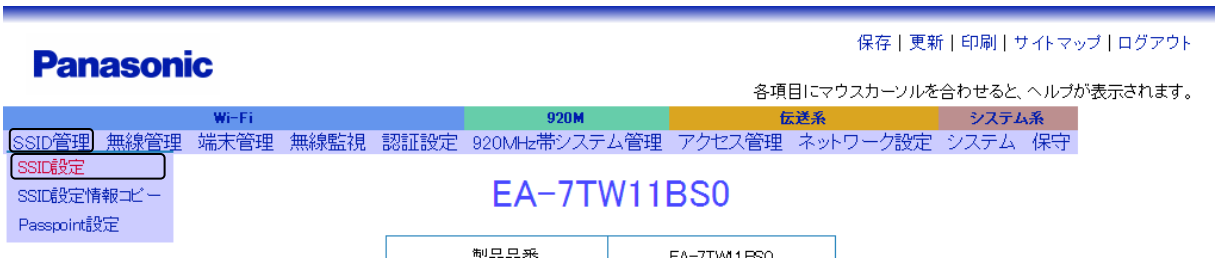


図4.1-10　メニュー（SSID 設定）

手順2　対象となる SSID の〔編集〕をクリックしクリックします。

図4.1-11　SSID 一覧

手順3　〔QoS〕をクリックします。

図4.1-12　SSID 編集（QoS）

手順4　〔WMM 規格に沿った QoS 制御〕を選択します。

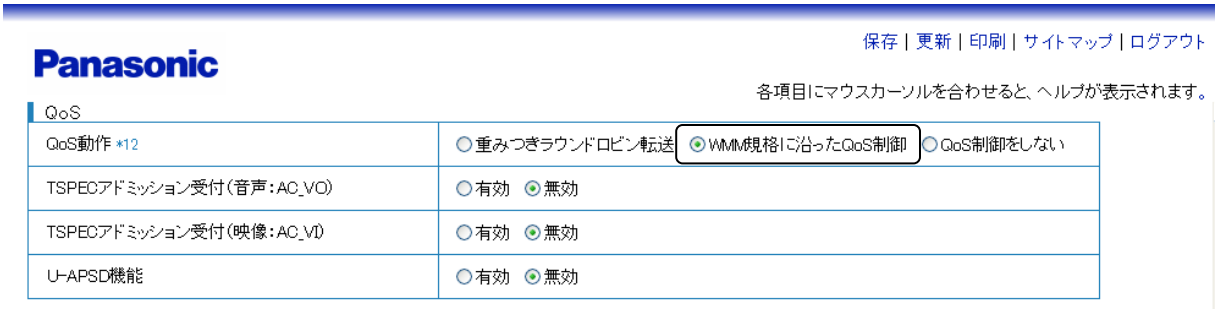


図4.1-13　QoS

手順5　画面最下部の〔設定〕をクリックし、設定を反映させます。

※VoIP 利用時に自動的に優先割り当てを行う簡易設定があります。「4.6.3　VoIP /Video 自動優先割り当て」を参照してください。

4.2 セキュリティ設定

コンセントレータは、無線 LAN サービスにおける認証・暗号化によるセキュリティ機能を備えています。認証および暗号化は、SSID ごとに設定できます。

4.2.1 認証と暗号化

コンセントレータでは、無線 LAN 環境のセキュリティを確保するために、セキュリティ機能（認証および暗号化）を備えています。SSID ごとに異なる暗号化を設定することはもちろん、同一 SSID 上に複数の暗号化方式を混在させることも可能です。これによって、ノート PC や VoIP 電話など、多彩な通信機器が存在する現在のオフィス環境のセキュリティにも対応できます。
本項では、コンセントレータに備えられている認証方式および暗号化方式の概要を紹介します。

■ 認証方式

認証とはマルチアクセス コンセントレータ を経由してネットワークに接続しようとするユーザのアクセス権を照合するための処理であり、無線 LAN のセキュリティ確保には不可欠な機能です。
コンセントレータが対応している認証方式には以下の 4 種類があります。

IEEE802.11 Authentication

IEEE802.11 標準が定める認証方式で、無線 LAN の接続要求時に行われます。認証方式には、open、shared、both（open と shared の両方をサポート）があります。他の認証方式との併用、または固定 WEP 以外の暗号化方式を利用する場合は、open を選択してください。

IEEE802.1X

IEEE802.1X 規格で定められた Authentication サーバを使用する認証方式です。IEEE802.1X での認証は無線クライアントと認証サーバで行われます。そして、認証後、無線クライアントには認証サーバが作成した鍵が安全に配送される（動的 WEP）ため、より安全な接続が確保されます。
なお、IEEE802.1X の認証サーバによる認証方式は、WPA や IEEE802.11i/WPA2 といった認証方式の中でも利用できます。

WPA

WPA は、「Wi-Fi Alliance」という米国の業界団体が定めた暗号化方式規格で、その中で認証方式も規定しています。Wi-Fi Alliance は、IEEE802.11i 標準策定前に、WEP の脆弱性を補った暗号方式である TKIP（Temporal Key Integrity Protocol）の仕様を切り出し、WPA として公開しました。
WPA が対応する認証方式には、PSK（事前共通鍵認証）と IEEE802.1X があります。

IEEE802.11i/WPA2

IEEE802.11i は、無線 LAN におけるセキュリティ標準を定める規格であり、先に WPA として切り出された仕様に、最新の暗号化形式である AES への対応を付け加えたものとなっています。
一方、WPA2 とは、Wi-Fi Alliance が公開した WPA の改良規格であり、IEEE802.11i に準拠しています。IEEE802.11i/WPA2 が対応する認証方式には、PSK（事前共通鍵認証）と IEEE802.1X があります。

■ **暗号化方式**

無線 LAN の場合、AP の電波を誰でも受信できてしまいます。傍受を防ぎ、安全な通信を確保するためには、送受信されるデータを暗号化する必要があります。
コンセントレータが対応している暗号化方式には以下の 3 種類があります。

WEP

RC4 というアルゴリズムに従った暗号化方式です。無線 LAN 端末とマルチアクセス コンセントレータに、固定的に WEP キーと呼ばれる暗号鍵を割り当てておく固定 WEP と、Authentication サーバでの認証後、サーバからダイナミックに WEP キーを割り当てる動的 WEP の 2 方式があります。固定 WEP は解読されやすく、非常に脆弱です。動的 WEP は、固定 WEP に比べてセキュリティは格段にアップしますが、動的 WEP を利用するためには Authentication サーバの設定が必要となります。

TKIP

WEP の暗号化アルゴリズムをベースとして、その脆弱性を補うために改良・強化された暗号化方式です。

CCMP

次世代暗号化標準（AES）を元にした、WEP や TKIP とはまったく別の強固な暗号化アルゴリズムを採用した暗号化方式です。

4.2.2　認証方式と暗号化方式の組み合わせ

セキュリティを設定する場合、認証方式と暗号化方式の両方を指定する必要があります。

■認証・暗号化の設定における共通操作

操作手順

手順1　〔Wi-Fi〕　→　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

図4.2-1　メニュー（SSID 設定）

手順2　対象となる SSID の〔編集〕をクリックしクリックします。

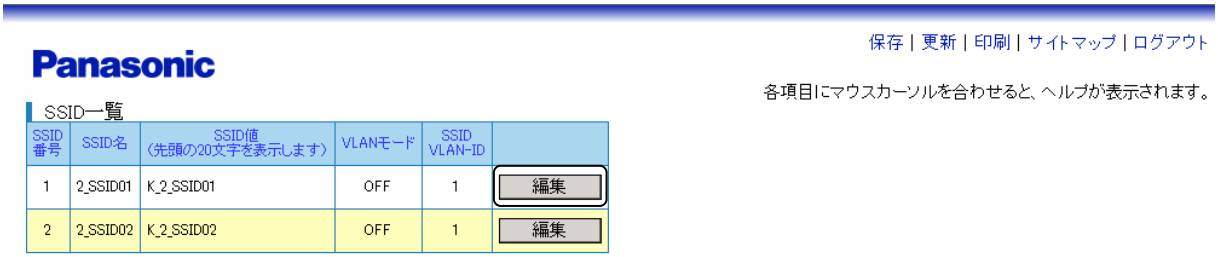


図4.2-2　SSID 一覧

以降の設定は、SSID 編集画面（図 4.2-3）より行います。

図4.2-3　SSID 編集

■IEEE802.11 設定

設定手順

手順1　〔SSID 編集〕画面（図 4.2-3）の〔IEEE802.11 設定〕をクリックします。
手順2　802.11 認証アルゴリズムの設定を行います。
固定 WEP 以外の暗号化方式を使用する場合は、必ず〔open〕を選択してください。
固定 WEP を使用する場合は、〔open〕、〔shared〕、〔両方〕のどれを選択してもかまいません。

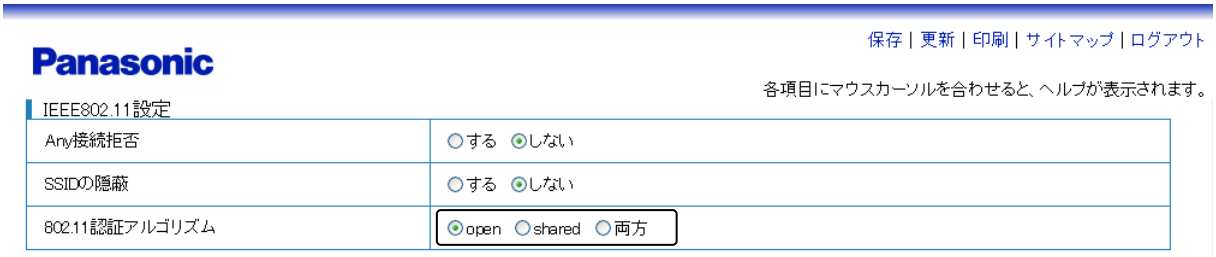


図4.2-4　IEEE802.11 設定

手順3　画面最下部の〔設定〕をクリックし、設定を反映させます。

■固定 WEP
暗号化方式として、固定 WEP を使用する場合は、以下の設定を行ってください。

設定手順

手順1　〔SSID 編集〕画面（図 4.2-3）の〔セキュリティ（共通）〕をクリックします。
手順2　固定 WEP に関する設定を行います。
例として、下記内容での設定を示します。
・ 固定 WEP〔有効〕を選択
・ WEP キー〔WEP40〕を選択
・ キー入力〔ASCII〕を選択し、キー値に「A1234」を入力

セキュリティ（共通）固定 WEP 選択

表4.2-1　動作モード一覧表

	鍵長	HEX	ASCII
WEP40	40bit	10 桁	5 文字
WEP104	104bit	26 桁	13 文字

手順3　画面最下部の〔設定〕をクリックし、設定を反映させます。

■動的 WEP

暗号化方式として、動的 WEP を使用する場合は、以下の設定を行ってください。

設定手順

手順1　〔SSID 編集〕画面（図 4.2-6）の〔セキュリティ（共通)〕をクリックします。

手順2　動的 WEP に関する設定を行います。

例として、下記内容での設定を示します。

・ 動的 WEP 〔有効〕を選択

・ WEP キー〔WEP40〕を選択

動的 WEP の場合、WEP キーの ASCII/HEX およびキーの設定は無視されます。

Authentication サーバの設定については「4.2.3 Authentication サーバを利用した IEEE802.1X 認証」を参照ください。

図4.2-5　セキュリティ（共通）動的 WEP 選択

手順3　画面最下部の〔設定〕をクリックし、設定を反映させます。

重要	■ 固定 WEP、動的 WEP をともに有効にした場合は、動的 WEP→固定 WEP の順で暗号化方式を試みます。

■WPA と TKIP

認証方式として WPA を選択し、暗号化方式として TKIP を PSK（Authentication サーバを使用しない）で利用する場合は、以下を設定してください。

設定手順

手順1　〔SSID 編集〕画面（図 4.2-6）の〔セキュリティ（共通）〕をクリックします。

手順2　WPA と TKIP に関する設定を行います。

例として、下記内容での設定を示します。

- WPA 〔有効〕を選択
- WPA/WPA2 認証方法〔PSK〕を選択
- TKIP 〔有効〕を選択

TKIP 有効の場合、各無線インターフェース設定画面の〔運用動作モード設定〕で、TKIP の〔有効〕を選択してください。

※この設定変更では、設定反映後の保存とリセットが必要となります。

- PSK〔パスフレーズ〕を選択し、暗号キーを入力

図4.2-6　セキュリティ（共通）WPA＋TKIP

表4.2-2　PSK 暗号キー入力一覧表

	入力可能文字数	入力可能文字
HEX	64 桁	16 進数
パスフレーズ	8～63 文字	半角英数字・半角記号（スペース、[?] は除く）

■WPA2 と TKIP、AES（CCMP）

認証方式として WPA2 を選択し、暗号化方式として TKIP と AES（CCMP） を Authentication サーバ使用で利用する場合は、以下を設定してください。

設定手順

手順1　〔SSID 編集〕画面（図 4.2-6）の〔セキュリティ（共通）〕をクリックします。

手順2　WPA2 と TKIP に関する設定を行います。

例として、下記内容での設定を示します。

・ WPA2 〔有効〕を選択

・ WPA/WPA2 認証方法〔802.1X〕を選択

・ TKIP の〔有効〕を選択

TKIP 有効の場合、各無線インターフェース設定画面の〔運用動作モード設定〕で、TKIP の〔有効〕を選択してください。

※この設定変更では、設定反映後の保存とリセットが必要となります。

・ AES 〔有効〕を選択

802.1X 認証を利用する場合、PSK の設定は無視されます。

「4.2.3 Authentication サーバを利用した IEEE802.1X 認証」を参照ください。

CCMP を利用するには、上記設定画面で AES を有効にします。

図4.2-7　セキュリティ（共通）WPA2＋TKIP

認証方式と暗号化方式の可能な組み合わせを以下の表に示します。なお、固定 WEP、動的 WEP、WPA（TKIP）、WPA2（TKIP）、WPA（CCMP）、WPA2（CCMP）を組み合わせて設定することで、同一 SSID 上に複数の認証方式・暗号化方式の端末を混在させることも可能です。

表4.2-3　認証方式と暗号化方式の組み合わせ一覧

IEEE802.11 認証 / 認証方式	Open 認証	Shared 認証
なし	固定 WEP	固定 WEP
IEEE802.1X	動的 WEP	×
WPA	TKIP	×
	CCMP	×
	TKIP と CCMP	×
IEEE802.11i/WPA2	TKIP	×
	CCMP	×
	TKIP と CCMP	×

※ WPA および WPA 2 の認証方式は、PSK、IEEE802.1X のいずれでもかまいません。

4.2.3　Authentication サーバを利用した IEEE802.1X 認証

IEEE802.1X 認証を使用するには、Authentication サーバの設定が必要です。コンセントレータでは、独立した IP インターフェースを 16 個持つことができ、各 IP インターフェースに Authentication サーバを 1 つずつ設定できます。（Authentication サーバ設定画面では、Web 認証と合わせて 32 個設定できます。）
以下に示す構成例では、SSID 名「SalesGroup」（SSID 値「SALES」）の認証方式に WPA2/IEEE802.1X が設定されています。ここでは、SSID 名「SalesGroup」を例に、IEEE802.1X 認証を利用し、Authentication サーバによってユーザを認証する方法を紹介します。

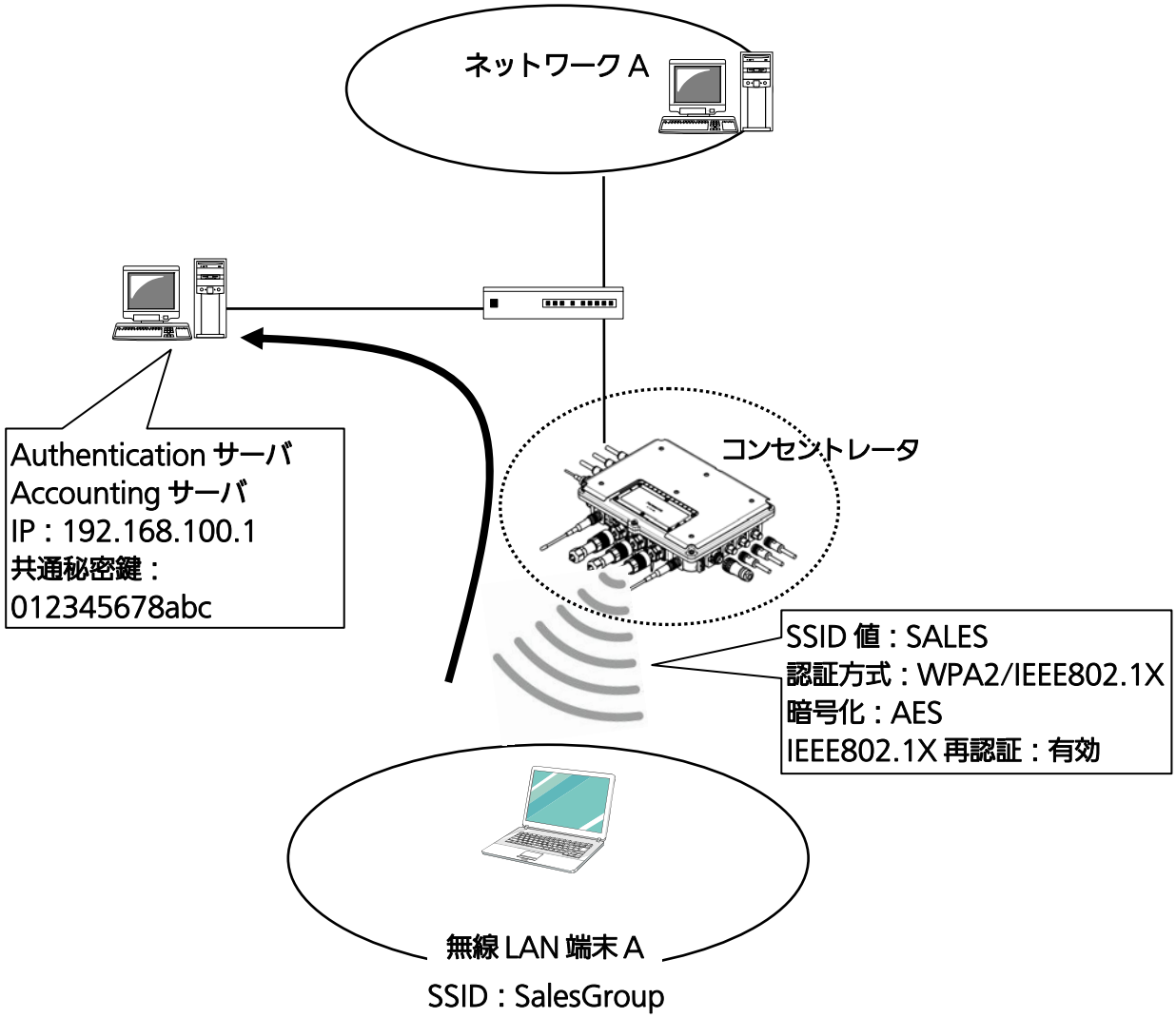


図4.2-8　　認証サーバを用いた環境構成例

設定手順

◆Authentication サーバの設定

手順1　〔Wi-Fi〕 → 〔認証設定〕 → 〔認証サーバ設定〕 → 〔Authentication サーバ設定〕をクリックします。

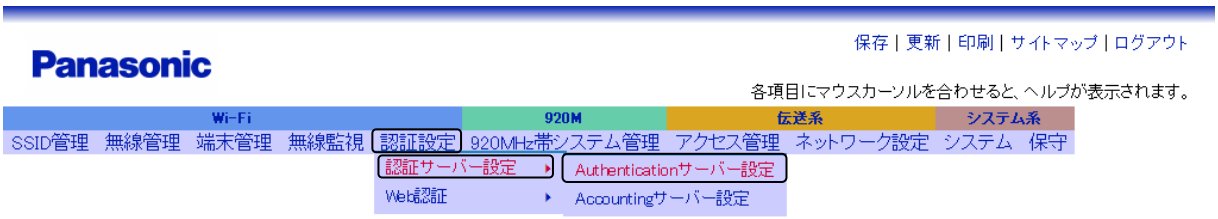


図4.2-9　メニュー（Authentication サーバ設定）

手順2　〔Authentication サーバー覧〕で設定するサーバグループ番号の〔編集〕をクリックします。
例として、サーバグループ番号：1 を選択します。

図4.2-10　Authentication サーバ設定

手順3　〔Running サーバ設定〕をクリックします。

図4.2-11　Authentication サーバ編集

手順4　Authentication サーバの設定を行います。

例として、下記内容での設定を示します。

- サーバ接続〔有効〕を選択
- サーバ名に「AUTH-01(MAIN)」を入力
- IP インターフェース番号〔1〕（Running サーバ接続に利用する自装置の IP インターフェース番号）を選択
- サーバ IP アドレスに「192.168.100.1」（Running サーバの IP アドレス）を入力
- 送信先ポート番号の〔1813〕（対象となる Running サーバの UDP ポート番号）を選択
- 共有秘密鍵に Running サーバの共有秘密鍵「012345678abc」を入力（1 ～ 64 文字、半角英数字と半角記号（〔?〕は除く））
- サーバによる端末制御〔有効〕を選択

図4.2-12　Running サーバ設定

手順5　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

※ Backup サーバを利用する場合は、Backup サーバに対しても同様の設定を行ってください。

◆Accounting サーバの設定

Accounting サーバも Authentication サーバとあわせて設置されている場合は、以下の手順で Accounting サーバの設定も行います。

手順6　〔Wi-Fi〕 → 〔認証設定〕 → 〔認証サーバ設定〕 → 〔Accounting サーバ設定〕をクリックします。

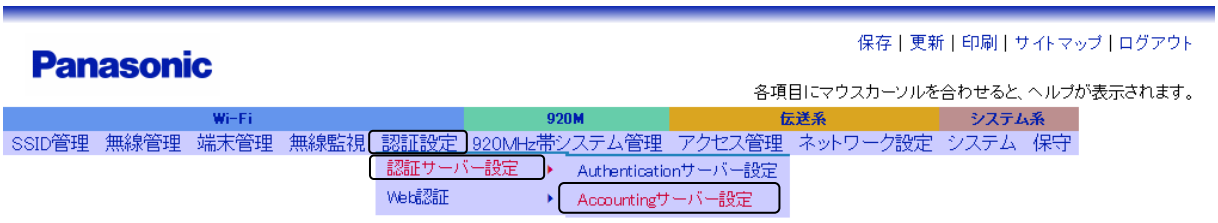


図4.2-13　メニュー（Accounting サーバ設定）

手順7　設定するサーバグループ番号の〔編集〕をクリックしクリックします。

例として、サーバグループ番号：1 を編集します。

図4.2-14　Accounting サーバ設定

手順8　〔Running サーバ設定〕をクリックします。

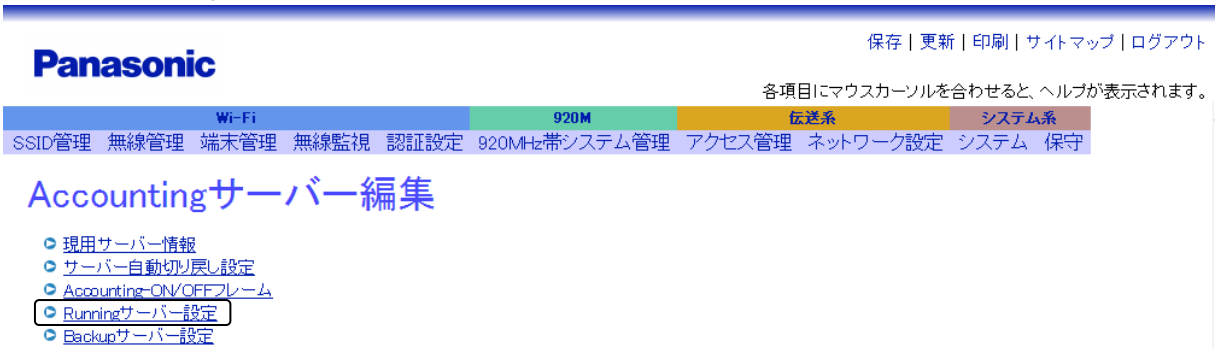


図4.2-15　Accounting サーバ編集

手順9　Accounting サーバの設定を行います。

例として、下記内容での設定を示します。

- サーバ接続の〔有効〕を選択
- サーバ名に「ACCT-01(MAIN)」を入力
- IP インターフェース番号〔1〕（Running サーバ接続に利用する自装置の IP インターフェース番号）を選択
- サーバ IP アドレスに「192.168.100.1」（Running サーバの IP アドレス）を入力
- 送信先ポート番号の〔1813〕（対象となる Running サーバの UDP ポート番号）を選択
- 共有秘密鍵に Running サーバの共有秘密鍵「012345678abc」を入力（1 ～ 64 文字、半角英数字と半角記号（〔?〕は除く））

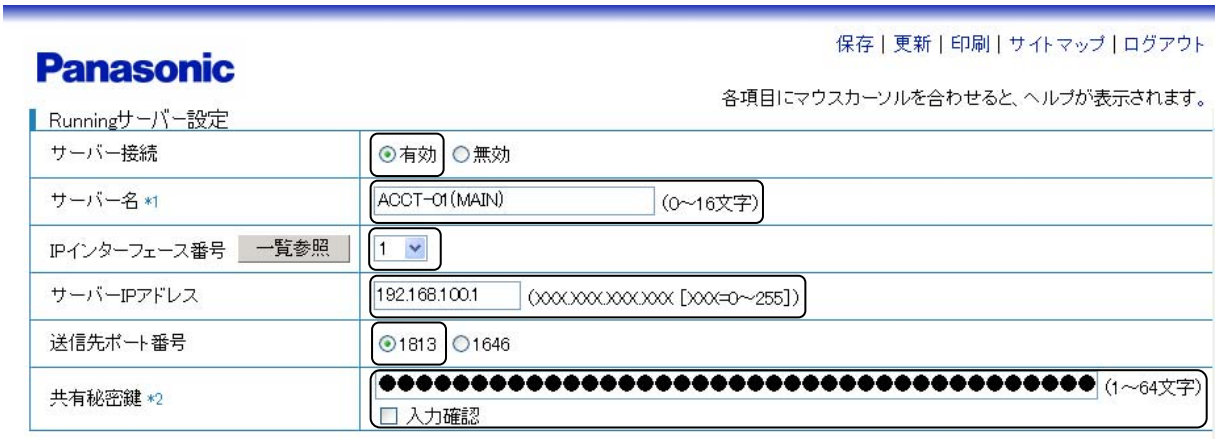


図4.2-16　Running サーバ設定

手順10　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

※ Backup サーバを利用する場合は、Backup サーバに対しても同様の設定を行ってください。

◆IEEE802.11i/WPA2 認証の設定

手順11 〔SSID 管理〕 → 〔SSID 設定〕を選択します。

図4.2-17 メニュー（SSID 設定）

手順12 対象となる SSID の〔編集〕をクリックします。

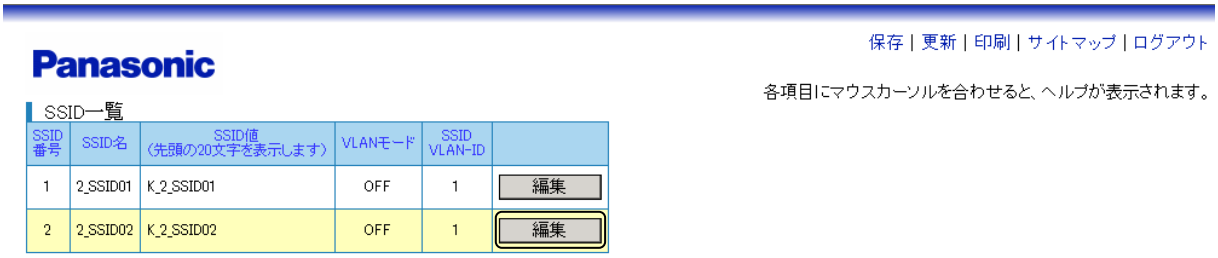


図4.2-18 SSID 一覧

手順13 〔IEEE802.11 設定〕をクリックします。

図4.2-19 SSID 編集（IEEE802.11 設定）

手順14　IEEE802.11 の設定を行います。

例として、802.11 認証アルゴリズム〔open〕を選択します。

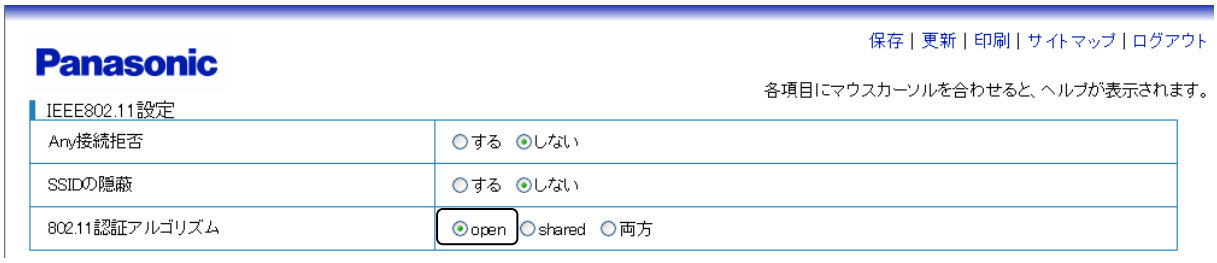


図4.2-20　IEEE802.11 設定

手順15　〔SSID 編集〕画面の〔セキュリティ（共通）〕をクリックし、WPA2 の設定を行います。

下記内容での設定を示します。

- WPA2 〔有効〕を選択
- WPA/WPA2 認証方法〔802.1X〕を選択
- AES 〔有効〕を選択

図4.2-21　セキュリティ（共通）

手順16　〔SSID 編集〕画面の〔IEEE802.1X 設定〕をクリックし、再認証実行を〔有効〕にします。

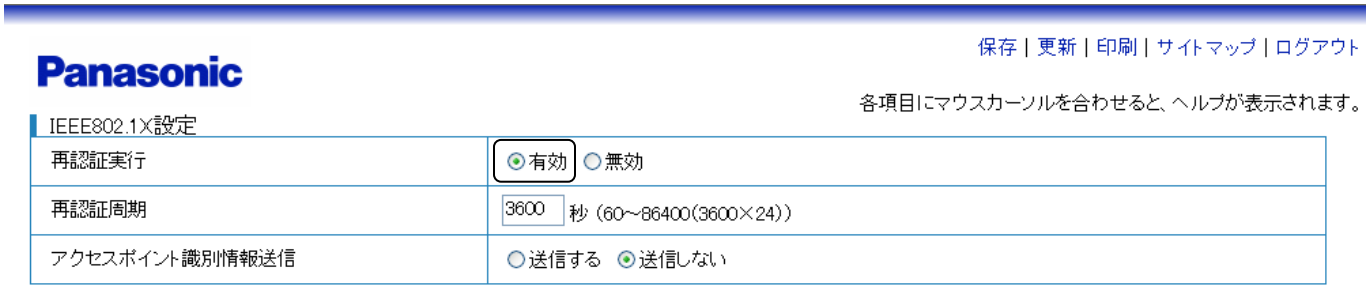


図4.2-22　IEEE802.1X 設定

手順17　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

◆SSID で使用する Authentication サーバの設定

手順18 〔SSID 編集〕画面の〔Authentication･Accounting（MAC 認証/EAP 認証)〕をクリックし、Authentication サーバの設定を行います。

例として、下記内容での設定を示します。

- 使用 Authentication サーバ番号に“1”（手順 2 で指定したサーバ番号）を選択
- NAS-ID に「nasidxxxx」を入力

図4.2-23 Authentication ･Accounting（MAC 認証/EAP 認証）

手順19 画面最下部の〔設定〕をクリックしクリックします。

以上で、Authentication サーバを使った WPA2 認証設定は完了です。

4.2.4　ユーザ認証

■ユーザ認証 VLAN

ユーザ認証 VLAN では、IEEE802.1X 認証により、無線 LAN 端末のユーザを基準にして、トラフィックを VLAN 分離することが可能となります。ここでは、以下の図に示すユーザ認証 VLAN ネットワークの設定方法を紹介します。

たとえば、ネットワーク A のユーザには、Authentication サーバによる認証の結果 VLAN-ID=100 が発行されて、ネットワーク A への接続が可能となります。また、ネットワーク B ユーザには、VLAN-ID=200 が発行され、ネットワーク B への接続が可能となります。

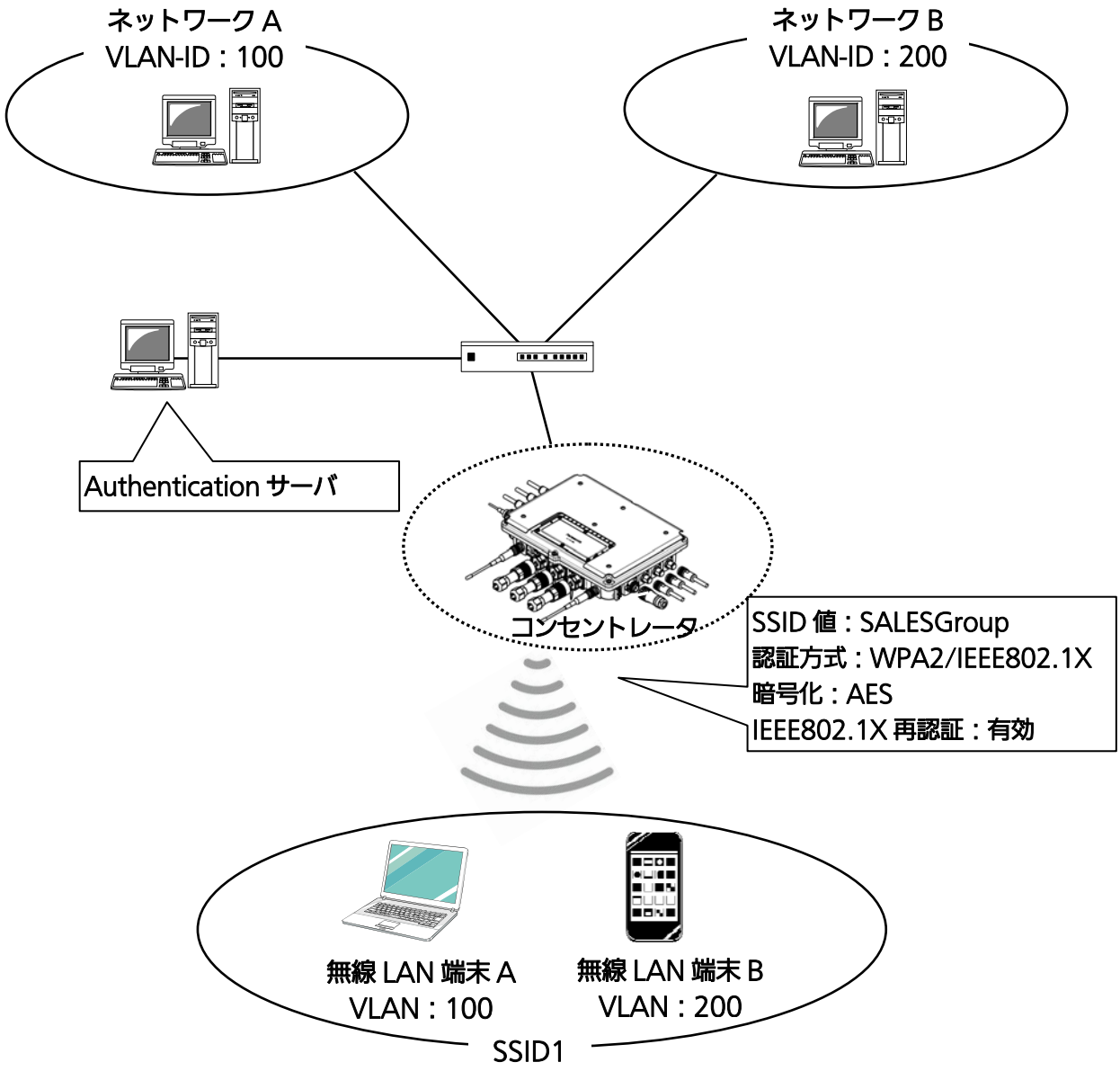


図4.2-24　環境例（ユーザ認証 VLAN）

Authentication サーバの設定方法については、「4.2.3　Authentication サーバを利用した IEEE802.1 認証」内の「■Authentication サーバ」を参照してください。

また、各ユーザに対して発行される VLAN-ID は、Authentication サーバ側にあらかじめ設定を行っておいてください。設定方法は、Authentication サーバの取扱説明書を参照してください。

◆〔SSID 編集〕画面の〔VLAN モード〕をクリックし、VLAN モードの設定を行います。
ユーザ認証 VLAN では、それぞれの VLAN 設定を行い、VLAN モードで〔User〕を選択します。
SSID の設定方法は、3.4 SSID の設定を参照してください。

図4.2-25　VLAN モード選択

以上で、ユーザ認証 VLAN の設定は完了です。

■ユーザ認証 VLAN ＋ SSID VLAN

SSID ごとに VLAN を分離したうえで、さらにユーザ認証 VLAN により無線 LAN 端末ごとに VLAN を分離することが可能となります。

ネットワーク A とネットワーク B とで VLAN 分離を行ったうえで、さらに管理用と一般用をユーザ認証 VLAN で分けるような設定が可能です。このような二重の VLAN 構成を実現するためには、SSID に対して拡張 VLAN（ダブルタグ VLAN）の設定を行ってください。

下記の構成例では、端末からのトラフィックは、はじめに SSID にマッピングされた VLAN-ID（100 or 200）によって部門ごとに分離された後、Authentication サーバによって割り当てられるユーザ認証 VLAN-ID（10 or 20）によって管理用ネットワークまたは一般用ネットワークのいずれかに分離されます。

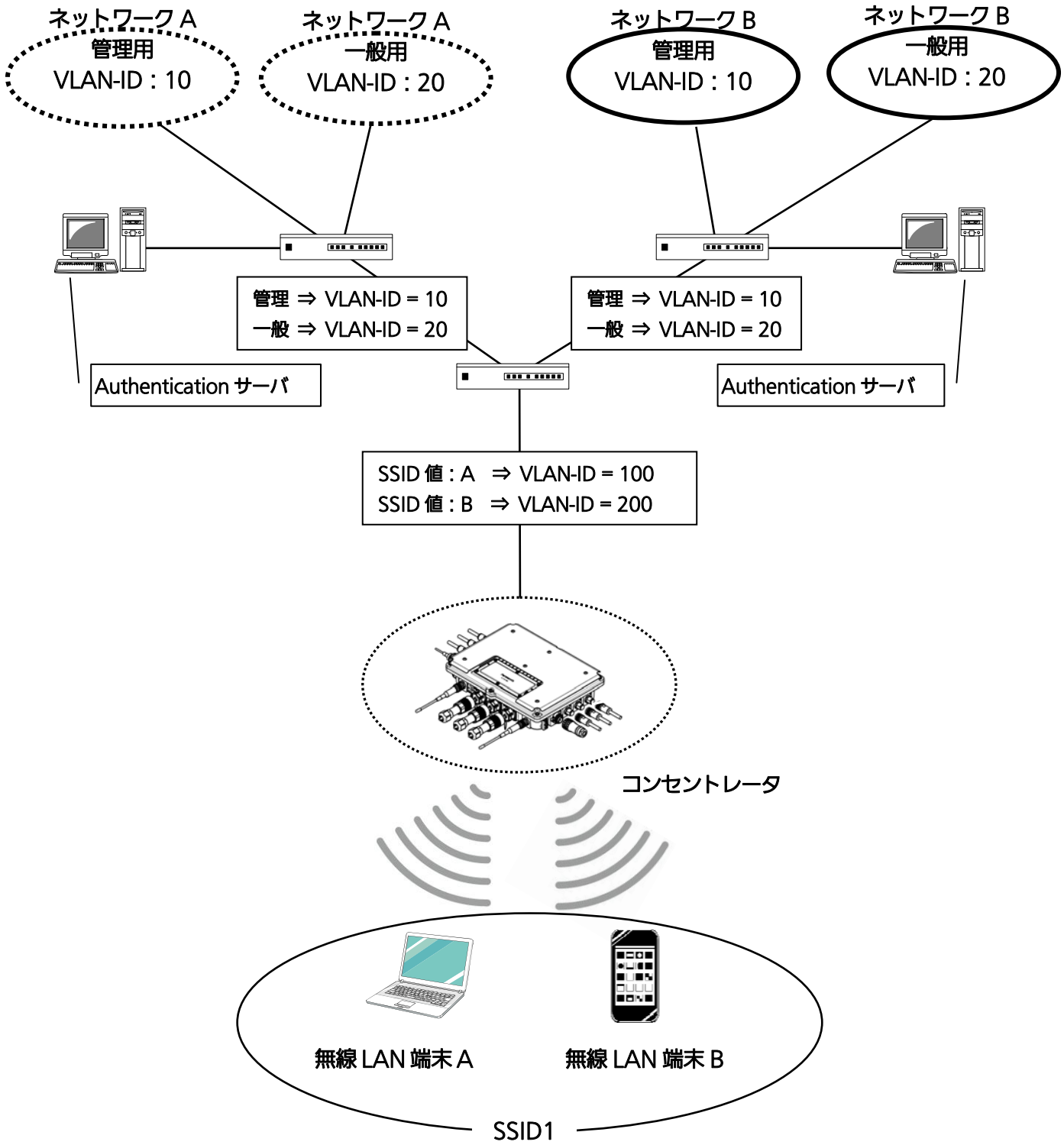


図4.2-26 構成例（ユーザ認証 VLAN ＋ SSID VLAN）

Authentication サーバの設定方法については、「4.2.3　Authentication サーバを利用した IEEE802.1X 認証」内の「■Authentication サーバ」を参照してください。
また、各ユーザに対して発行される VLAN-ID は、Authentication サーバ側にあらかじめ設定を行っておいてください。

ユーザ認証 VLAN ＋ SSID VLAN では、それぞれの VLAN 設定を行い、VLAN モードで〔SSID ＆ User〕を選択します。

図4.2-27 VLAN モード（SSID 設定）

以上で、ユーザ認証 VLAN ＋ SSID VLAN の設定は完了です。

4.3　自動干渉回避

コンセントレータでは、無線伝送路の干渉状態を観測し、得られた結果をもとに送受信チャネルを自動的に選択・変更して干渉を回避することができます。

送受信チャネルの自動選択の場合、干渉が観測されても、すぐに干渉の自動回避が行われるわけではなく、特定の電界強度以上の状態が 6 分間以上続くと干渉ありと判断されます。その後 特定の電界強度以下の状態が 6 分間以上続くと、干渉なしと判断されます。
（特定の電界強度：干渉波＝－60 dBm、干渉 AP＝－70 dBm ）

4.3.1　無線監視設定

無線監視機能に関する設定を行います。

設定手順

◆無線監視の設定

手順1　〔Wi-Fi〕　→　〔無線監視〕　→　〔無線監視設定〕を選択します。

図4.3-1 メニュー（無線監視設定）

手順2　無線監視に関するパラメーターの変更を行います。

干渉検出用 RSSI レベル、干渉検出用 Noise レベル、干渉検出時の検出監視時間干渉検出時の干渉復旧時間、干渉情報リスト追加監視回数設定を変更することが可能です。

図4.3-2 無線監視設定

4.3.2　送受信チャネル自動変更

4.9GHz 帯の設定を例に、送受信チャネルの自動変更の設定方法を紹介します。

設定手順

◆送受信チャネルの自動変更の設定

ここではインターフェース（IF1）設定を例に説明します。

手順1　〔Wi-Fi〕　→　〔無線管理〕　→　〔インターフェース（IF1）設定〕を選択します。

図4.3-3 メニュー（インターフェース（IF1）設定）

手順 2 ～ 手順 4 は〔インターフェース（IF1）設定〕画面（図 4.3-2）より各種設定を行います。

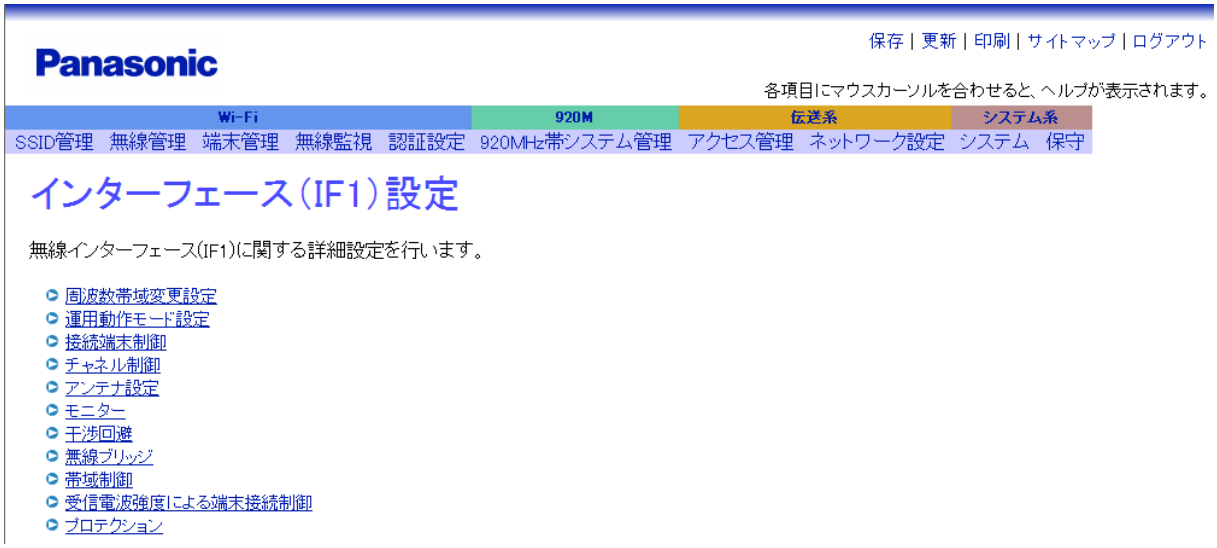


図4.3-4　インターフェース（IF1）設定

手順2　〔インターフェース（IF1）設定〕画面（図 4.3-2）の〔運用動作モード設定〕をクリックし、無線インターフェースの動作と動作モードを設定します。

例として、下記内容での設定を示します。

- 無線インターフェース〔有効〕を選択
- 動作モード〔通常運用〕を選択
  ※動作モードの設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

〔無線モニタ〕を選択した場合、そのマルチアクセス コンセントレータへの端末接続はできなくなり、監視のみが行われます。

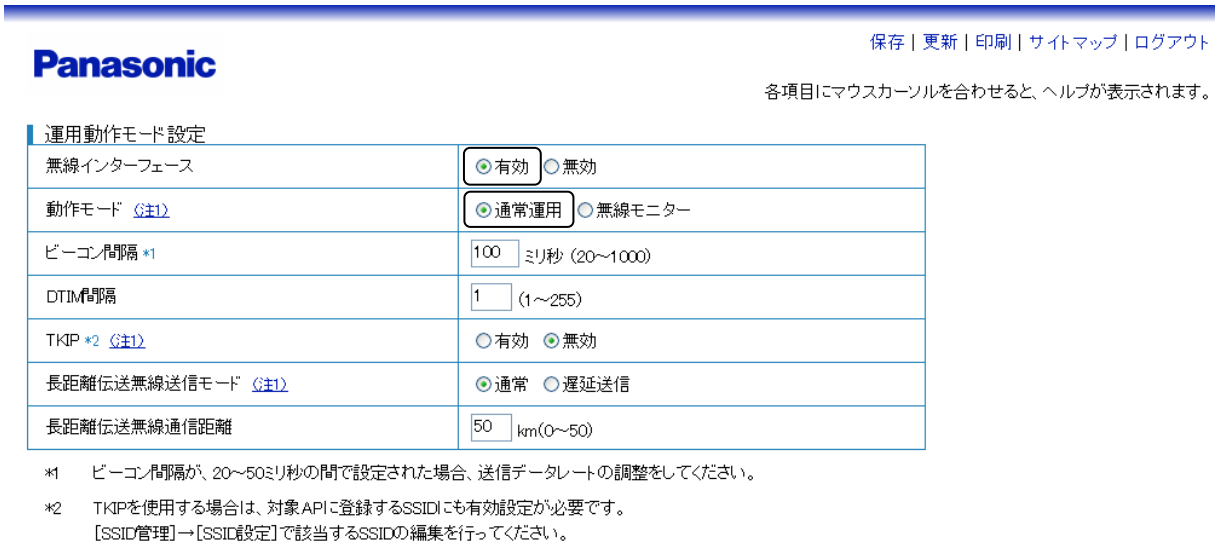


図4.3-5 運用動作モード設定

手順3　〔インターフェース（IF1）設定〕画面(図 4.3-4)の〔チャネル制御〕をクリックし、チャネル制御モードと固定（優先）チャネル番号（4.9GHz）と選択可能チャネル（4.9GHz）を設定します。

例として、下記内容での設定を示します。

- チャネル制御モード：〔自動〕を選択
- チャネル番号：〔192〕を選択
- 選択可能チャネル（184h ～ 196ch）：〔選択可能にする〕を選択

図4.3-6　チャネル制御

手順4　〔インターフェース（IF1）設定〕画面（図 4.3-4）の〔干渉回避〕をクリックし、干渉検出時最終動作を選択します。

例として、干渉検出時最終動作の〔スタンバイ〕を選択します。

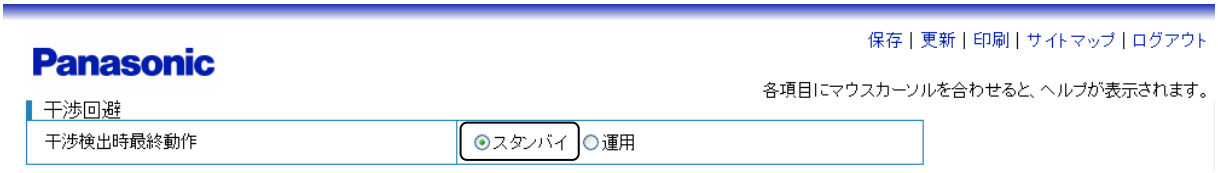


図4.3-7　干渉回避

手順5　画面最下部の〔設定〕をクリックします。

※他システムからの干渉検出時の最終動作には、以下の 2 種類があります。
・スタンバイ：利用可能周波数がないためモニタ動作を行う。
・運用： 一番影響の少ない周波数を選択して動作を続ける。
また、無線中継モード（無線ブリッジ）を使用すると、クライアント AP はその無線インターフェースでの自動干渉回避はできません（サーバ AP は自動干渉回避します）。

4.3.3　隣接 AP・干渉 AP の確認

コンセントレータは、使用チャネルの「常時監視」（スタンバイ、もしくは監視モードである場合は、全チャネルの「常時監視」）を行います。監視の結果は各種状態として表示するとともに、これを元に干渉検出・干渉回避、レーダー検出・回避などの処理を行います。
2.4GHz 帯の無線インターフェースでは 1ch～13ch、4.9GHz 帯の無線インターフェースでは 184ch～196ch、5GHz 帯の無線インターフェースでは 100ch～140ch を監視します。

操作手順

◆隣接 AP

手順1　〔Wi-Fi〕　→　〔無線監視〕　→　〔隣接 AP〕を選択します。

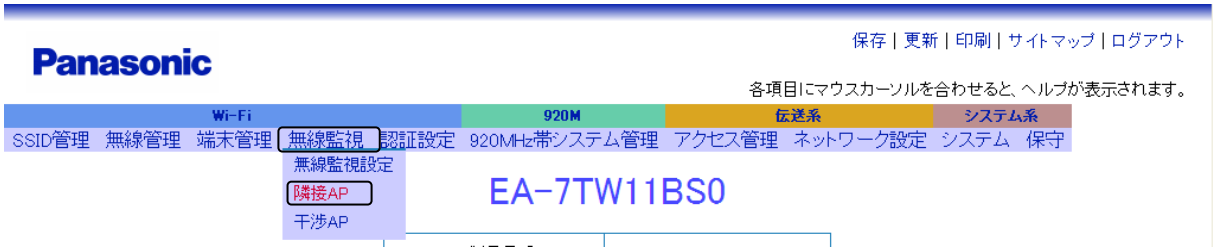


図4.3-8　メニュー（隣接 AP）

手順 2 ～ 手順 6 は〔隣接 AP〕画面（図 4.3-7）より各種操作を行います。

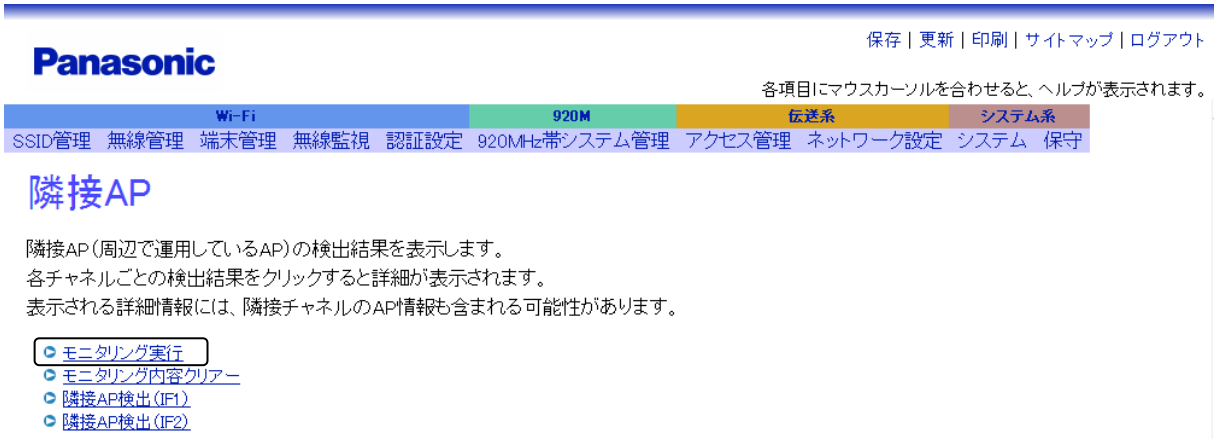


図4.3-9　隣接 AP

手順2　〔隣接 AP〕画面(図 4.3-7)にて、モニタリング実行をクリックし、〔実行〕をクリックします。

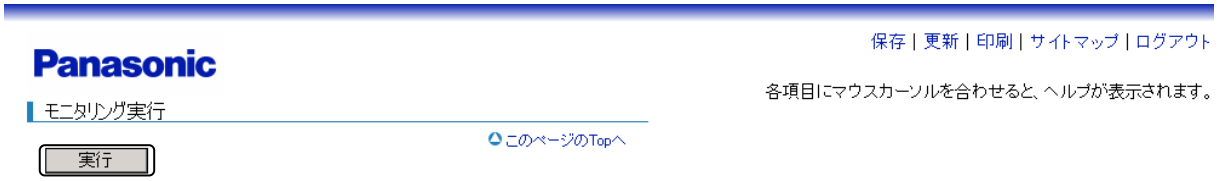


図4.3-10　モニタリング実行

手順3　〔モニタリング実行確認〕のダイアログボックスで〔OK〕をクリックします。

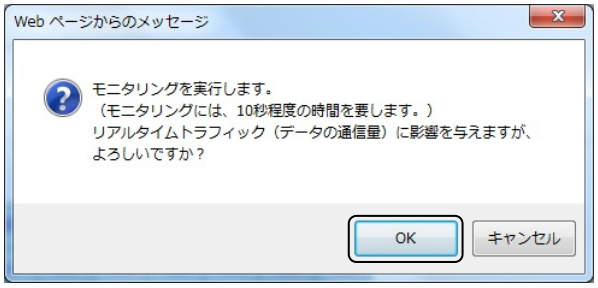


図4.3-11　モニタリング実行確認

手順4　〔モニタリング実行受付〕のダイアログボックスで〔OK〕をクリックします。

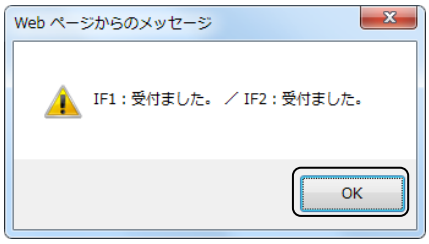


図4.3-12　モニタリング実行受付

手順5　手順 5 〔隣接 AP〕画面（図 4.3-7）にて、〔隣接 AP 検出（IF1)〕または〔隣接 AP 検出（IF2)〕をクリックします。

手順6　隣接 AP 検出結果欄の“〇”または“ - ”をクリックします。（図 4.3-11）
ここでは、4.9GHz 帯無線インターフェースを例にとり説明します。

図4.3-13　隣接 AP 検出

手順 6 で隣接 AP 検出結果欄の“〇”または“ - ”をクリックすると、下記画面（図 4.3-12）が表示されます。

図4.3-14　隣接 AP モニタリング結果

◆干渉 AP

手順1　〔Wi-Fi〕　→　〔無線監視〕　→　〔干渉 AP〕を選択します。

図4.3-15　メニュー（干渉 AP）

手順2　〔干渉 AP 検出（IF1）〕または〔干渉 AP 検出（IF2）〕をクリックします。

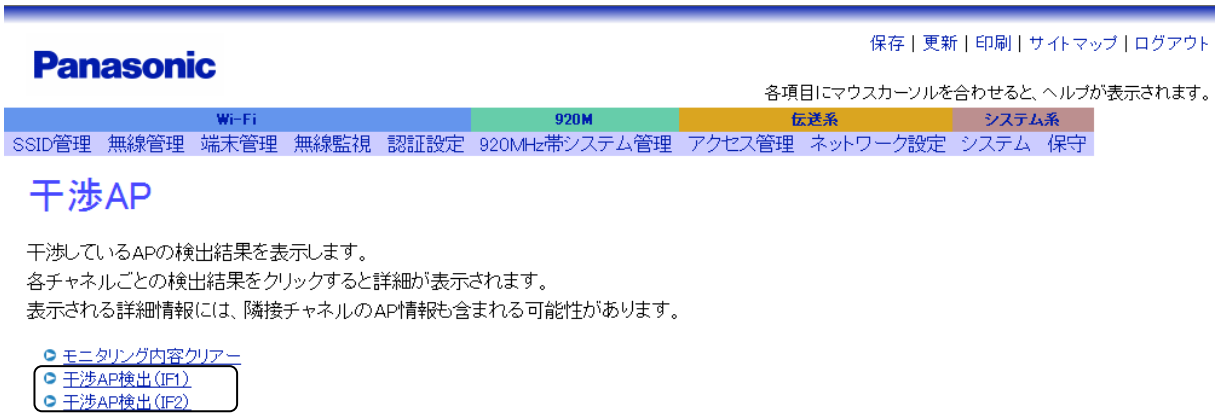


図4.3-16　干渉 AP

手順3　干渉 AP 検出結果欄の“〇”または“ - ”をクリックします。

図4.3-17　干渉 AP 検出

手順 3 で干渉 AP 検出結果欄をクリックすると、下記画面（図 4.3-16）が表示されます。

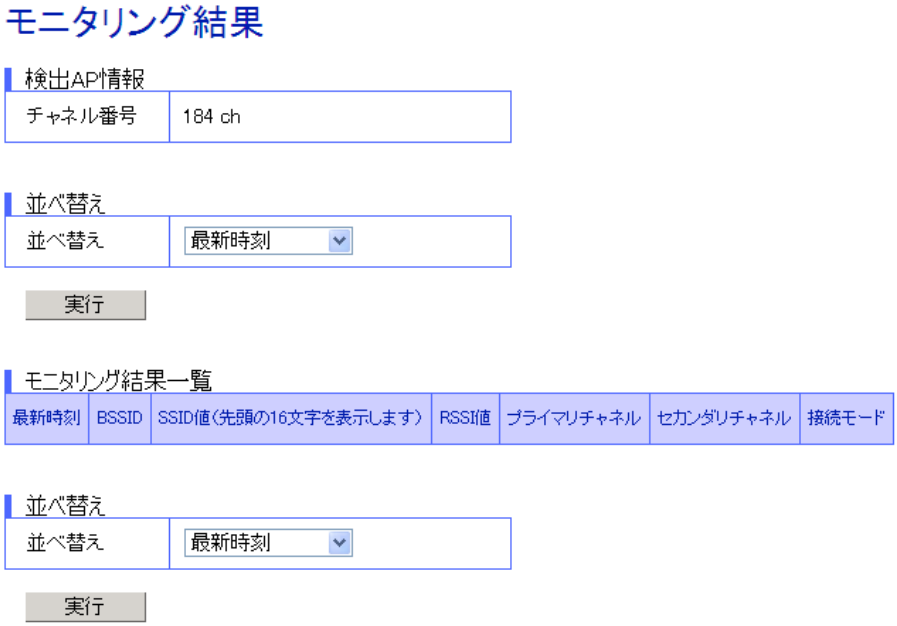


図4.3-18　干渉 AP モニタリング結果

4.3.4 レーダー監視

レーダー監視の概要

コンセントレータは、各種レーダーと共用する 5.47～5.725GHz（W56）のチャネルに対応しているため、各種レーダーを監視する機能を備えています。5GHz 帯の無線インターフェースで 100,104,108,112,116,120,124,128, 132,136,140 チャネル（以下、レーダー監視対象チャネル）を設定した場合、レーダー監視機能（起動時･運用中の動作）を自動的に動作させます。

起動時の動作

装置の起動時にレーダー監視対象チャネルのいずれかが選択されていた場合、各種レーダー波検出を 1 分間行います。各種レーダーを検出した場合は、TRAP にて通知を行い（設定がされていた場合のみ）、適切な送受信チャネルを選択し自動変更します。選択されたチャネルもレーダー監視対象チャネルのいずれかである場合は、同様に 1 分間のレーダー確認を行い、以後これを繰り返し、最終的にレーダーが検出されないチャネルを選択します。

送受信チャネルが固定で設定されていた場合、最終動作設定が「強制送信」設定でも、レーダー波検出後 30 分間のスタンバイ状態になります。30 分後に改めて起動時の動作を行います。

また、装置の起動時に本機能が動作するため、装置が動作するまでに約 2 分程度時間がかかります。

運用中の動作

各種レーダーが検出されずレーダー監視対象チャネルのいずれかのチャネルで運用を開始したとしても、その使用チャネルでの各種レーダー波検出を行います。各種レーダー波を検出した場合、TRAP にて通知を行い（設定がされていた場合のみ）、そのマルチアクセス コンセントレータ配下のすべての端末に Deauthentication を送信し端末の切断を行って、起動時と同様の動作をします。

5GHz 帯の無線インターフェースでレーダー監視対象チャネルを設定した場合、本機能は自動的に有効になります。設定を変更することはできません。

4.3.5　周波数帯域幅復旧

周波数帯域幅が 20 MHz /40MHz に設定されている場合に、チャネル選択時もしくは、セカンダリチャネル側のレーダー検出もしくは、セカンダリチャネル側の干渉波検出により、周波数帯域幅が 20MHz に決定した場合は、「40MHz 復旧幅監視間隔」ごとに、チャネル選択を実施し、20 MHz /40MHz で運用可能な周波数を検索します。

ただし、「周波数自動制御」設定が固定で、運用周波数が 140ch の場合は、20/40MHz 運用できないため、「40MHz 復旧幅監視間隔」にかかわらず、復旧処理は行いません。

4.9GHz 帯および 5GHz 帯で 40MHz 運用が可能なため本設定は 4.9GHz 帯および 5GHz 帯を選択したインターフェースで有効化されます。

設定手順

◆周波数帯域幅復旧設定

手順1　〔Wi-Fi〕　→　〔無線管理〕　→　〔インターフェース（IF2）設定〕を選択します。

図4.3-17　メニュー（インターフェース（IF2）設定）

手順2　〔チャネル制御〕をクリックします。

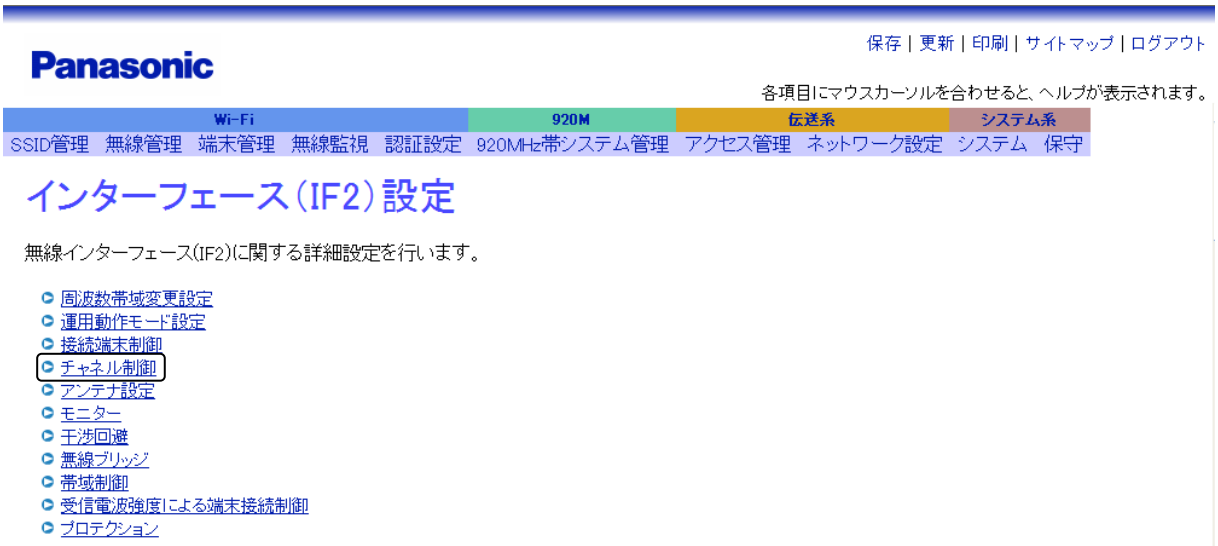


図4.3-18　インターフェース（IF2）設定

手順3　〔チャネル制御モード〕、〔周波数帯域幅〕、〔40MHz 復旧監視機能〕、〔40MHz 復旧監視間隔〕を設定します。

例として、下記内容での設定を示します。

- チャネル制御モード　　：〔自動〕を選択
- 周波数帯域幅　　：〔20MHz/40MHz〕を選択
- 40MHz 復旧監視機能　　：〔有効〕を選択
- 40MHz 復旧監視間隔　　：「30」分を入力

※ 40MHz 復旧監視機能を[有効]にした場合、モニタ機能（3.6　各無線インターフェースの設定参照）と同様の動作を行うため、パケットロスが発生したり、接続した端末が切断される可能性があります。

図4.3-19　チャネル制御（5GHz）

手順4　画面最下部の〔設定〕をクリックし、設定を反映させます。

4.4　フィルタリング

コンセントレータでは、ユーザからのデータフレーム（無線 LAN 端末への無線 LAN 送信フレームおよび、無線 LAN 端末からの無線 LAN 受信フレーム、マルチアクセス コンセントレータからの無線ブリッジフレームおよび、マルチアクセス コンセントレータへの無線ブリッジフレーム、マルチアクセス コンセントレータへの受信 Ether フレーム）に対して、MAC レイヤーでのフィルタリング、IP レイヤーでのフィルタリングを行うことができます。
また、ユーザデータのフィルタリングとは別に、管理用 IP インターフェースごとに、管理フレーム（Admin フレーム：装置宛てのフレーム）をフィルタリングすることもできます。

■ブリッジフィルター条件
以下の条件を基に、MAC レイヤーのフィルタリング条件（アクセスリスト）が設定できます。アクセスリストは 512 個設定することができます。

① イーサタイプ
② 送信元 MAC アドレス
③ 送信先 MAC アドレス
④ VLAN-ID
⑤ CoS 値（802.1p プライオリティ）（=/</>の指定可能）

上記条件の破棄・透過の設定を複数エントリーすることが可能です。
①～⑤の各条件に対してすべてを受け入れる指定も可能です。

■IP フィルター条件
以下の条件を基に、IP レイヤーのフィルタリング条件（アクセスリスト）適用の有無が設定できます。
アクセスリストは 512 個設定することができます。

① IP プロトコル種別
② 送信元ネットワークアドレス
　フルアドレスマスクにより　ホストの指定も可能（マスクは中抜き可能）
③ 宛先ネットワークアドレス
　フルアドレスマスクにより　ホストの指定も可能（マスクは中抜き可能）
④ 送信元 UDP／TCP ポート番号（=/</>の指定可能）
⑤ 送信先 UDP／TCP ポート番号（=/</>の指定可能）
⑥ TOS 値（=/</>の指定可能）

上記条件の破棄・透過の設定を複数エントリーすることが可能です。
①～⑥の各条件に対してすべてを受け入れる指定も可能です。

■PPPoE フィルター条件
PPPoE フレームへの IP レイヤーフィルタリング条件（アクセスリスト）が設定できます。SSID 単位、もしくは無線ブリッジ時における VLAN-ID 単位で設定が可能です。

ここでは、無線 LAN 端末からの無線 LAN 受信フィルター設定を説明します。

設定手順

◆フィルター設定（ブリッジフィルター条件）

手順1　〔伝送系〕 → 〔アクセス管理〕 → 〔アクセス制御リスト編集〕 → 〔ブリッジ条件設定〕を選択します。

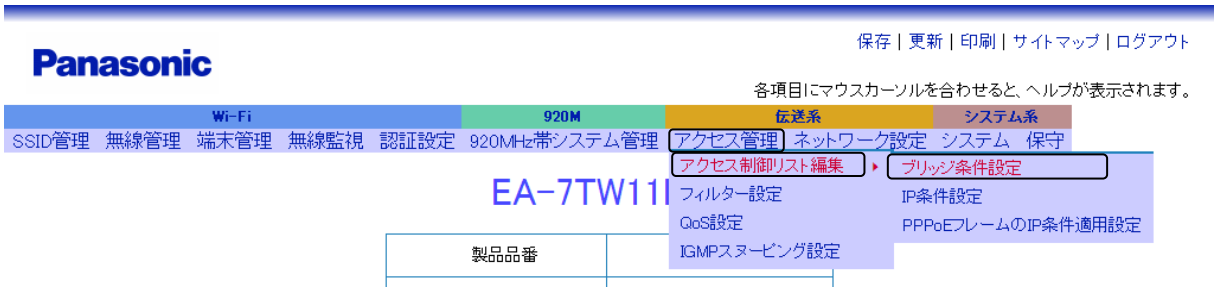


図4.4-1 メニュー（ブリッジ条件設定）

手順2　〔編集〕をクリックします。

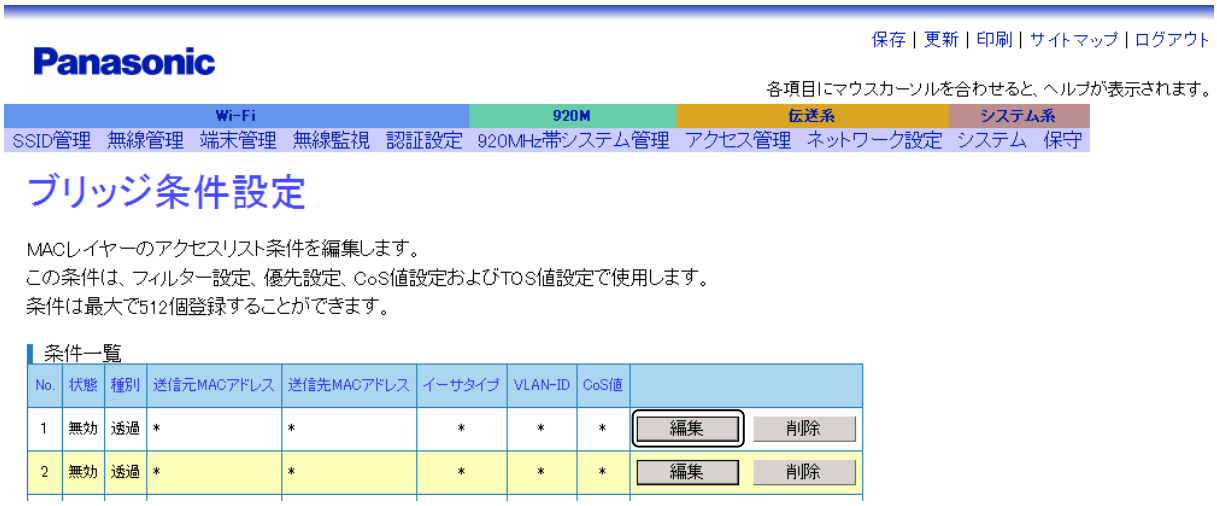


図4.4-2　ブリッジ条件設定

手順3　ブリッジ条件を登録します。

例として、下記内容での設定を示します。

- 実施種別に〔破棄〕を選択（下記条件に合ったものを破棄します。）
- 送信元 MAC アドレスは、「11-00-00-11-12-2C」を入力
- 送信先 MAC アドレスは、「00-0D-56-C1-11-DA」を入力
- イーサタイプは「CCCC」を入力
- VLAN-ID は「1」を入力
- CoS 値は「=7」を入力

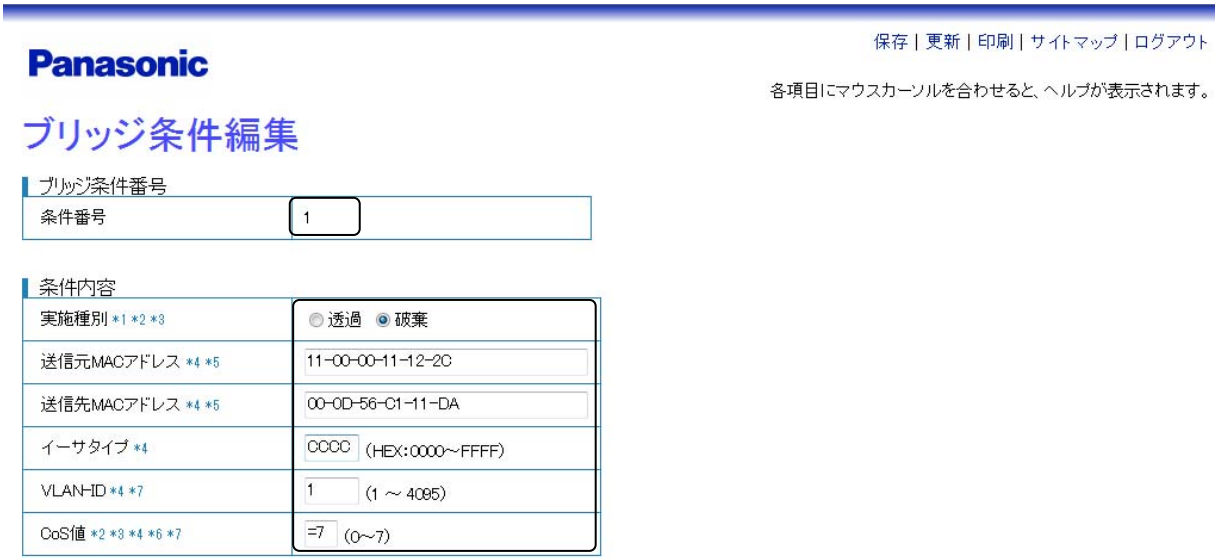


図4.4-3　ブリッジ条件編集

手順4　画面最下部の〔設定〕をクリックします。

手順5　〔伝送系〕　→　〔アクセス管理〕　→　〔フィルター設定〕　を選択します。

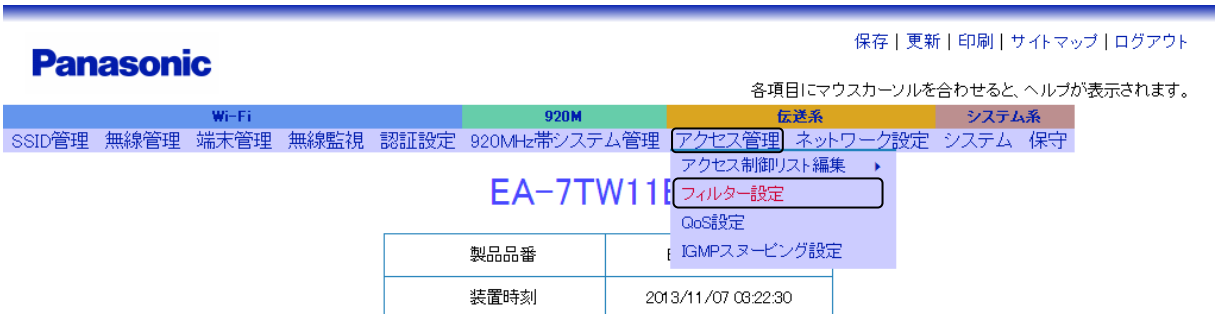


図4.4-4　メニュー（フィルター設定）

手順6　〔Ethernet ポート受信〕をクリックしたのち、〔Ethernet ポート受信〕選択で
〔ブリッジ条件〕をクリックします。

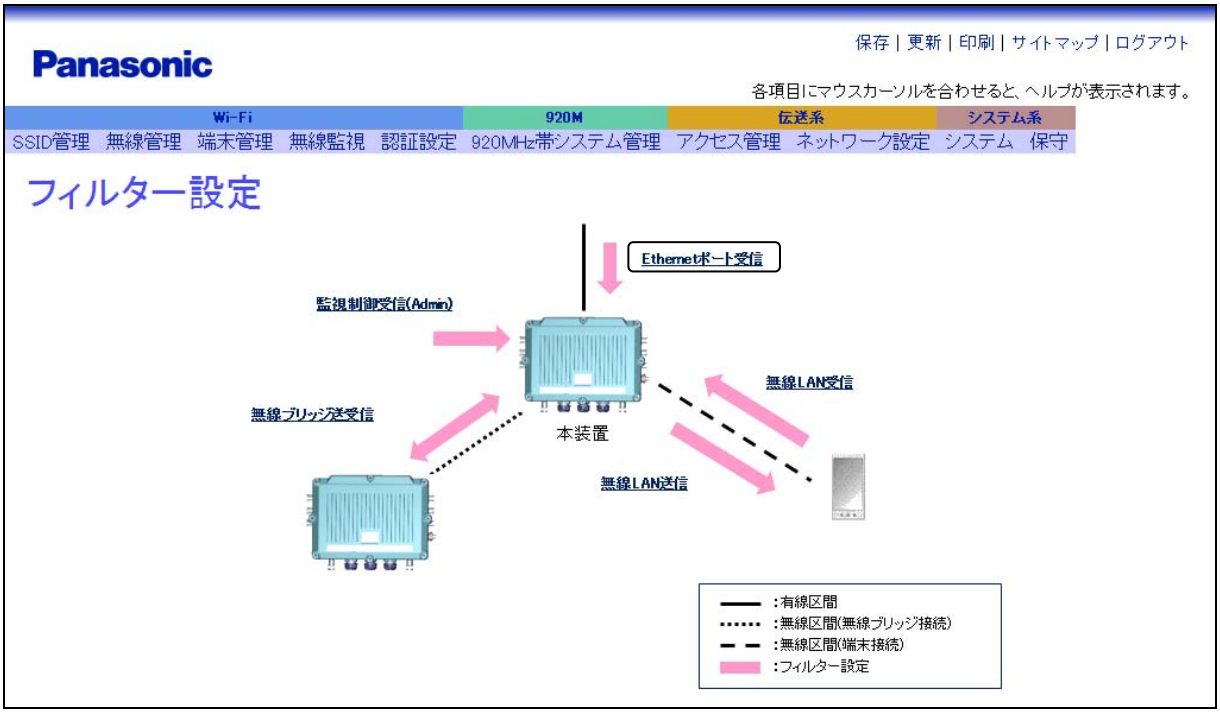


図4.4-5　フィルター設定(Ethernet ポート受信)

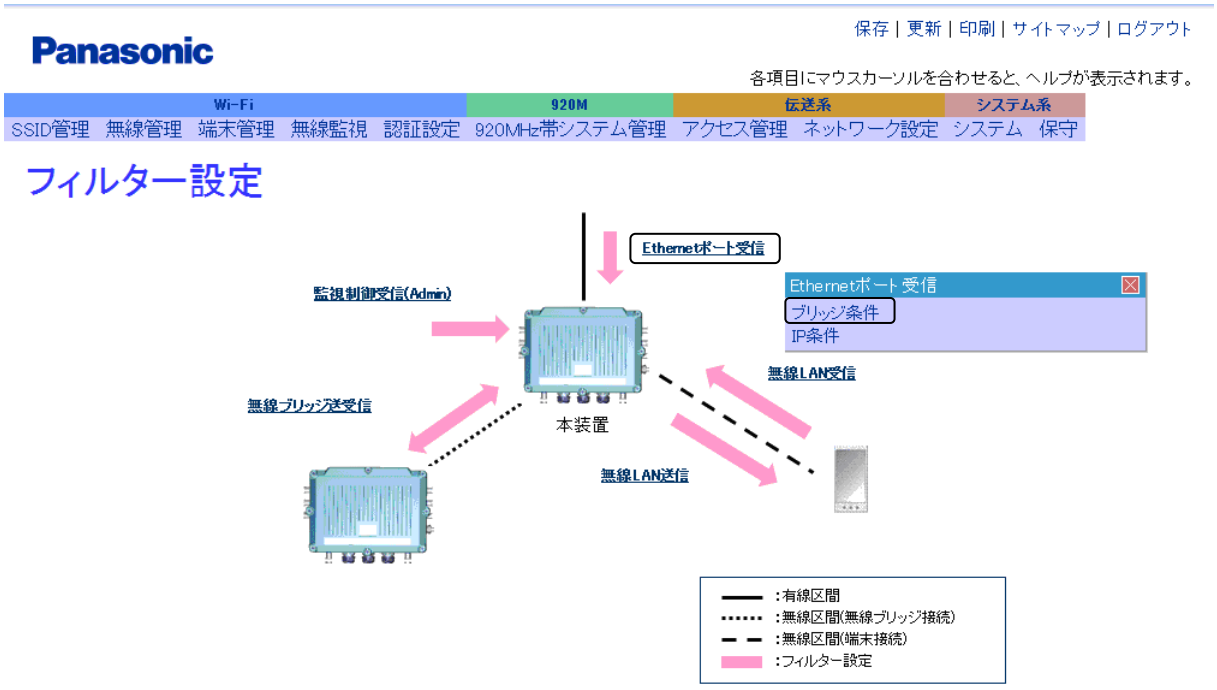


図4.4-6　フィルター設定(Ethernet ポート受信 ブリッジ条件)

手順7　ブリッジフィルター設定する SSID 番号をドロップダウンリストから選択し、〔表示〕をクリックします。

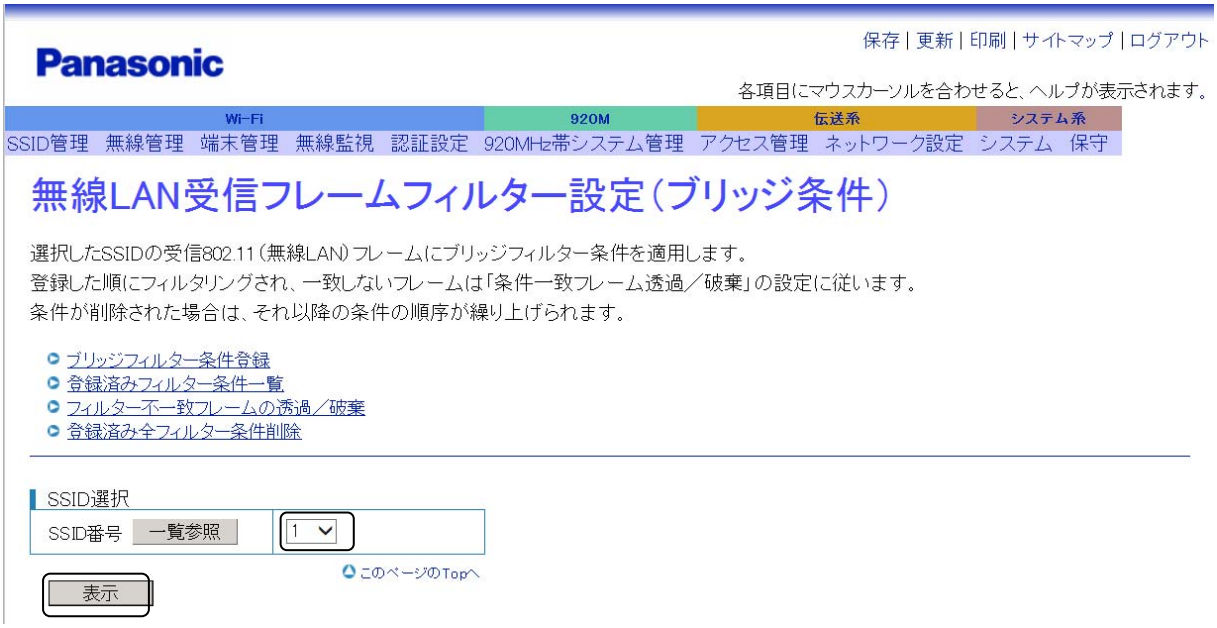


図4.4-7　SSID 選択

手順 7 で〔表示〕をクリックすると、下記画面が表示されます。(図 4.4-8)

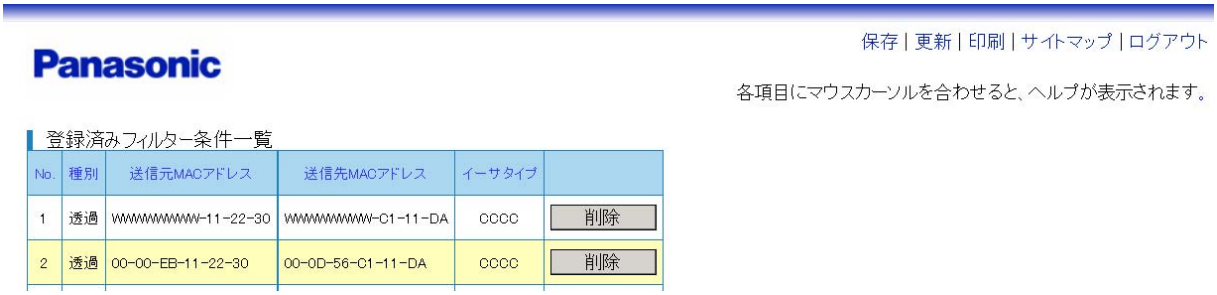


図4.4-8　登録済みフィルター条件一覧

手順8　ブリッジフィルター条件番号を入力し、〔登録〕をクリックします。

図4.4-9　ブリッジフィルター条件登録

◆フィルター設定（IP フィルター条件）

手順1　〔伝送系〕　→　〔アクセス管理〕　→　〔アクセス制御リスト編集〕　→　〔IP 条件設定〕を選択します。

図4.4-10　メニュー（IP 条件設定）

手順2　〔編集〕をクリックします。

Panasonic
保存 | 更新 | 印刷 | サイトマップ | ログアウト
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
Wi-Fi
920M
伝送系
システム系
SSID管理 無線管理 端末管理 無線監視 認証設定 920MHz帯システム管理 アクセス管理 ネットワーク設定 システム 保守
IP条件設定
IPレイヤーのアクセスリスト条件を編集します。
この条件は、フィルター設定、優先設定、CoS値設定およびTOS値設定で使用します。
条件は最大で512個登録することができます。
条件一覧
No. 状態 種別 送信元IPアドレス 送信元IPマスク値 送信先IPアドレス 送信先IPマスク値 TOS プロトコル 送信元ポート 送信先ポート
1 無効 透過 * * * * * * * * 編集 削除
2 無効 透過 * * * * * * * * 編集 削除

図4.4-11　IP 条件設定

手順3　IP 条件を登録します。

例として、下記内容での設定を示します。

- 実施種別に〔破棄〕を選択（下記条件に合ったものを破棄します。）
- 送信元 IP アドレスは、「192.168.100.254」を入力
- 送信元 IP マスク値は、「255.255.255.0」を入力
- 送信先 IP アドレスは、「192.168.100.100」を入力
- 送信先 IP マスク値は、「255.255.255.0」を入力
- TOS 値は「=60」を入力
- プロトコル番号は「239」を入力
- 送信元ポート番号は「<65530」を入力
- 送信先ポート番号は「>65535」を入力

図4.4-12 IP 条件編集

手順4　画面最下部の〔設定〕をクリックします。

手順5　〔伝送系〕　→　〔アクセス管理〕　→　〔フィルター設定〕を選択します。

図4.4-13　メニュー（アクセス管理）

手順6　〔無線 LAN 受信〕をクリックしたのち、〔無線 LAN 受信〕選択で〔IP 条件〕をクリックします。

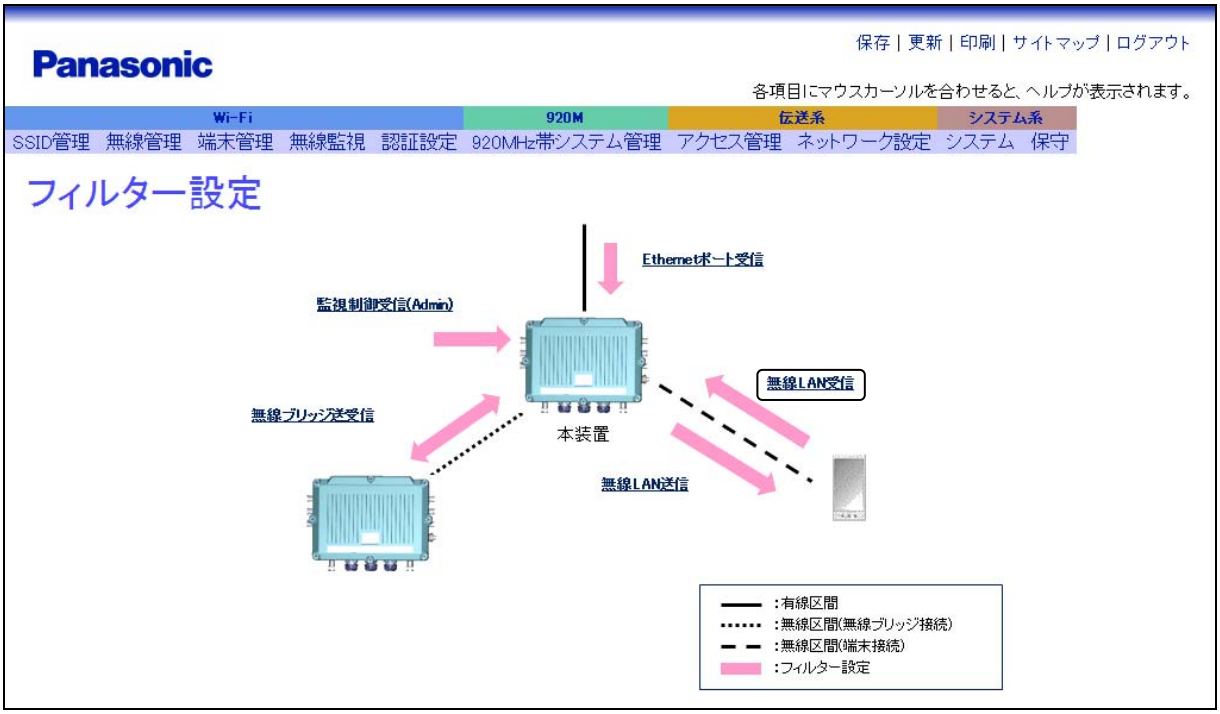


図4.4-14　フィルター設定(マルチアクセス コンセントレータ)

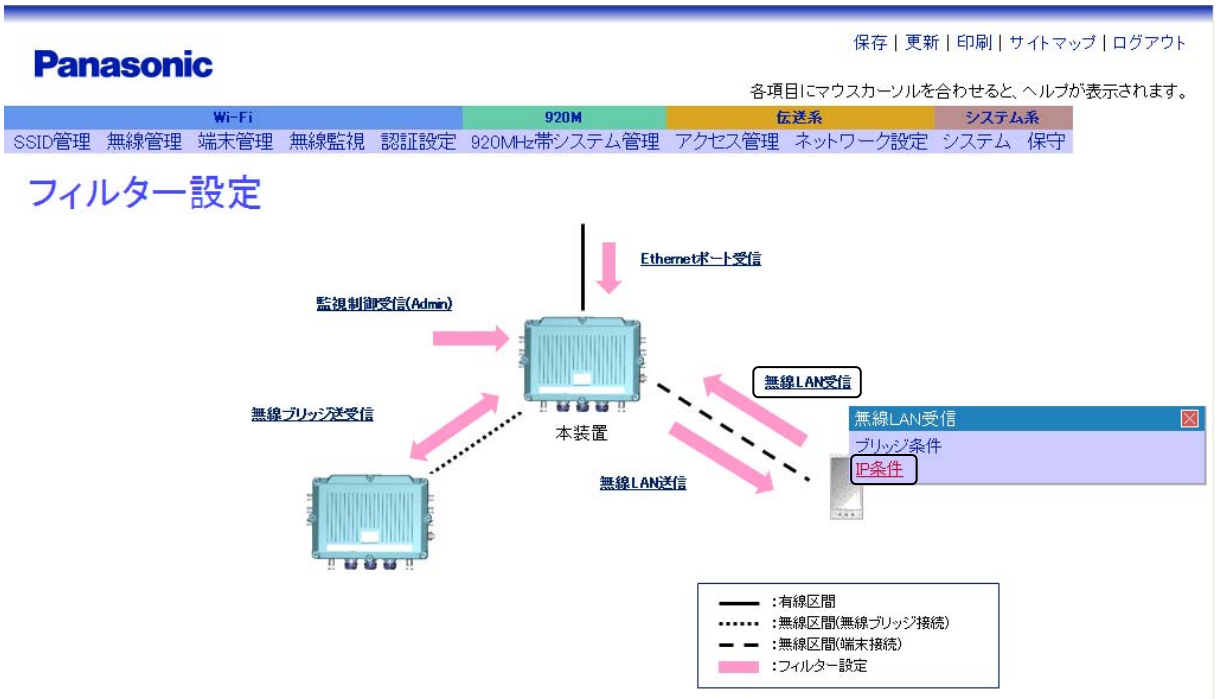


図4.4-15　フィルター設定(マルチアクセス コンセントレータ)

手順7　IP フィルター設定する SSID 番号をドロップダウンリストから選択し、〔表示〕をクリックします。

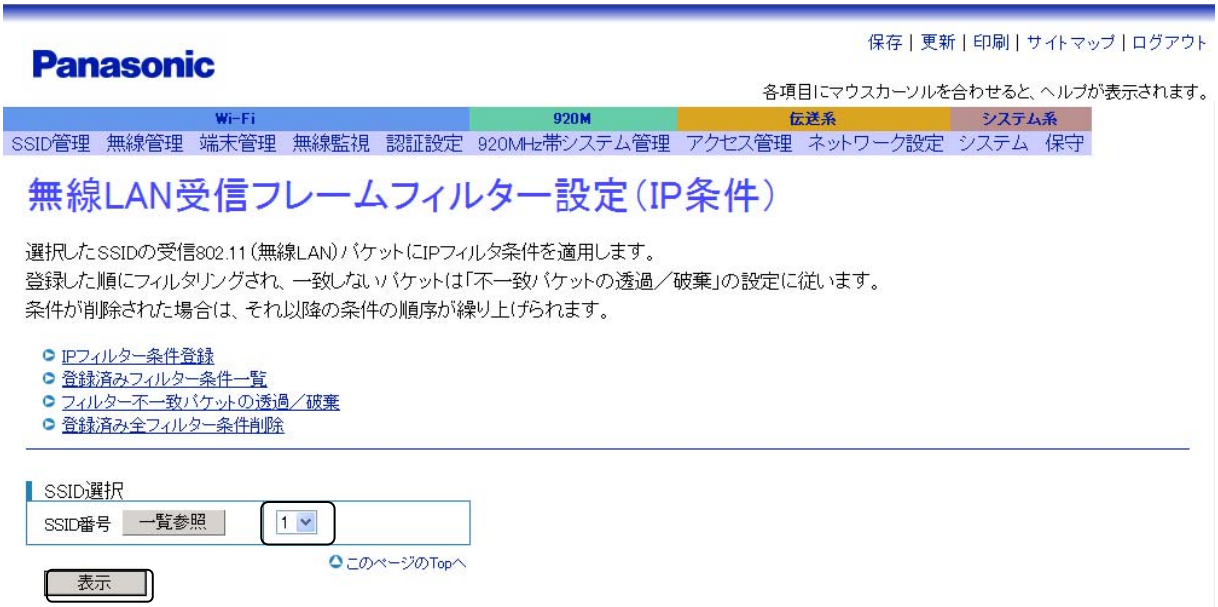


図4.4-16　SSID 選択

手順 7 で〔表示〕をクリックすると、下記画面が表示されます。（図 4.4-17）

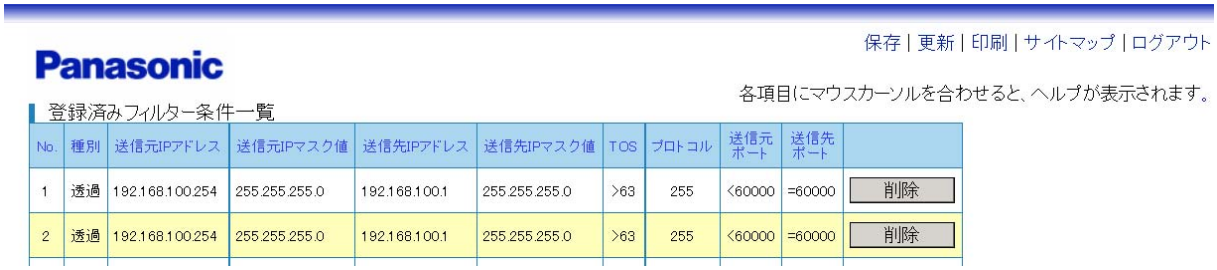


図4.4-17　登録済みフィルター条件一覧

手順8　IP フィルター条件番号を入力し、〔登録〕をクリックする。

図4.4-18　IP フィルター条件登録

◆フィルター設定（PPPoE フィルター条件）

例として IP 条件設定を行った後、PPPoE フィルター条件を設定する方法を説明します。

IP 条件設定手順は、「◆フィルター設定（IP フィルター条件）」 の手順 1 ～ 手順 3 を参照ください。

手順1　〔伝送系〕　→　〔アクセス管理〕　→　〔アクセス制御リスト編集〕
→　〔PPPoE フレームの IP 条件適用設定〕を選択します。

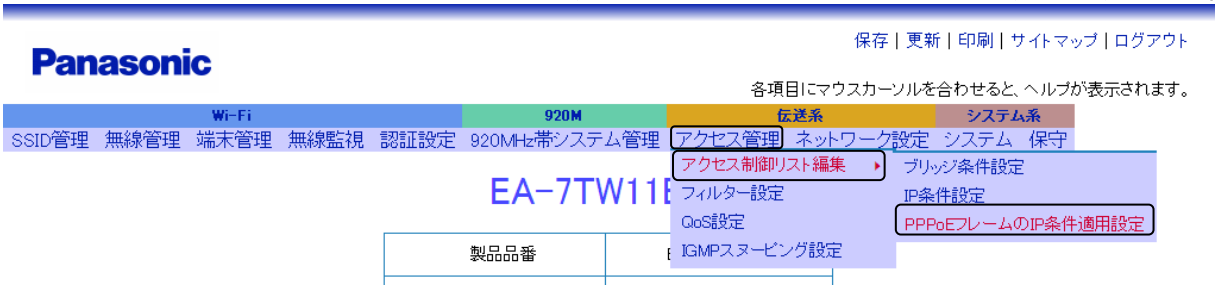


図4.4-19　メニュー（PPPoE フレームの IP 条件適用設定）

手順2　〔PPPoE フレームの IP 条件適用設定〕をクリックします。

図4.4-20　PPPoE フレームの IP 条件適用設定

手順3　PPPoE フレームの IP 条件適用設定を行う。

例として、下記内容での設定を示します。

・ SSID 番号〔1〕を選択

・ IP 条件を適用する（〔適用させる〕を選択）

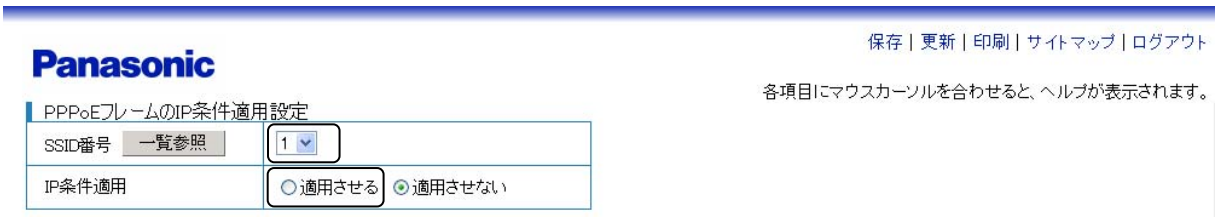


図4.4-21　PPPoE フレームの IP 条件適用設定

PPPoE フレームの Ethernet 用アクセスフィルター設定は、〔PPPoE フレームの条件適用設定（Ether)〕にて行います。図 4.4-22 では、Ether ポート 1 に適用した場合を示します。

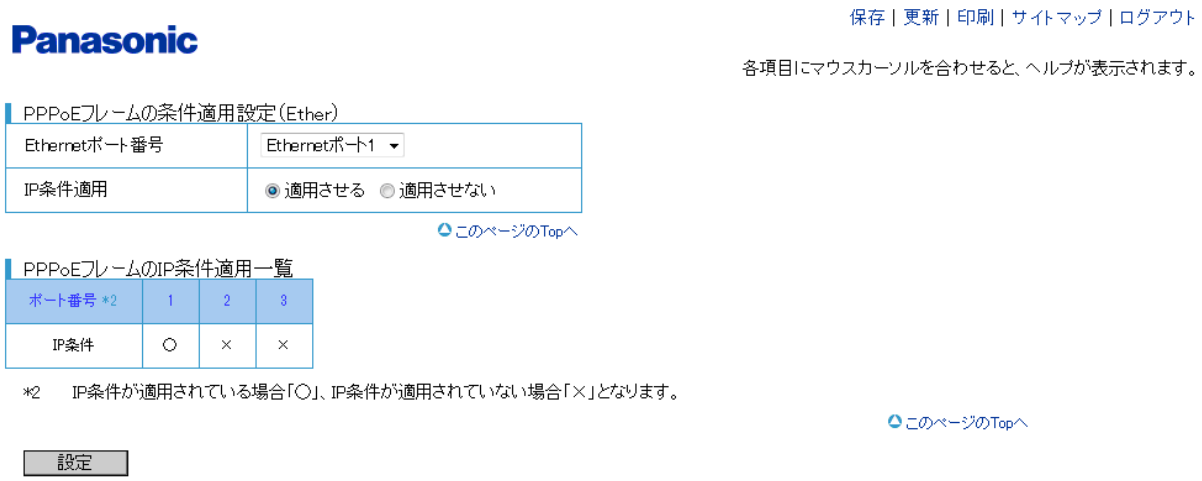


図4.4-22　PPPoE フレームの条件適用設定（Ether）

PPPoE フレームの無線ブリッジ用アクセスフィルター設定は、〔PPPoE フレームの VLAN-ID 条件適用設定〕にて行います。（図 4.4-23）

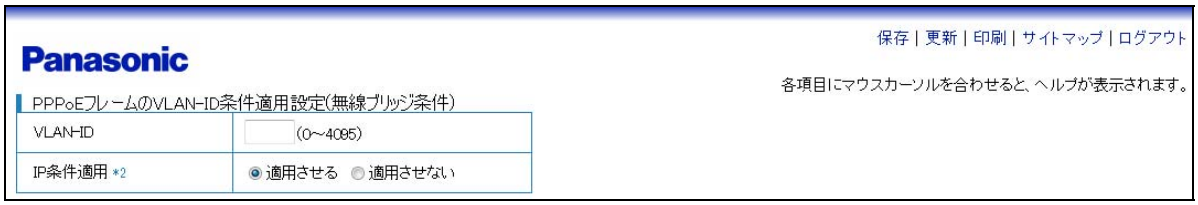


図4.4-23　PPPoE フレームの VLAN-ID 条件適用設定（無線ブリッジ条件）

手順4　画面最下部の〔設定〕をクリックします。

4.5　無線ブリッジ

無線ブリッジ機能を利用して、コンセントレータ同士を無線多段接続することで、無線 LAN エリアを拡充できます。無線ブリッジ接続したコンセントレータは、Ethernet ケーブルで直接接続した場合と同様に機能します。
中継接続する場合、被接続側のコンセントレータをサーバ側コンセントレータ、接続を行うコンセントレータをクライアント側コンセントレータとして設定します。サーバ側コンセントレータ 1 台の無線インターフェースごとに最大 64 台（64 分岐）のクライアント側コンセントレータを接続することが可能です。段数についての制限はありません。
また、コンセントレータと無線 LAN 端末間の WMM® (Wi-Fi Multimedia ™) による QoS 制御に加えて、無線ブリッジ接続時でも QoS 制御が可能です。

ここでは、下の図に示すような多段接続を行うための設定方法を紹介します。

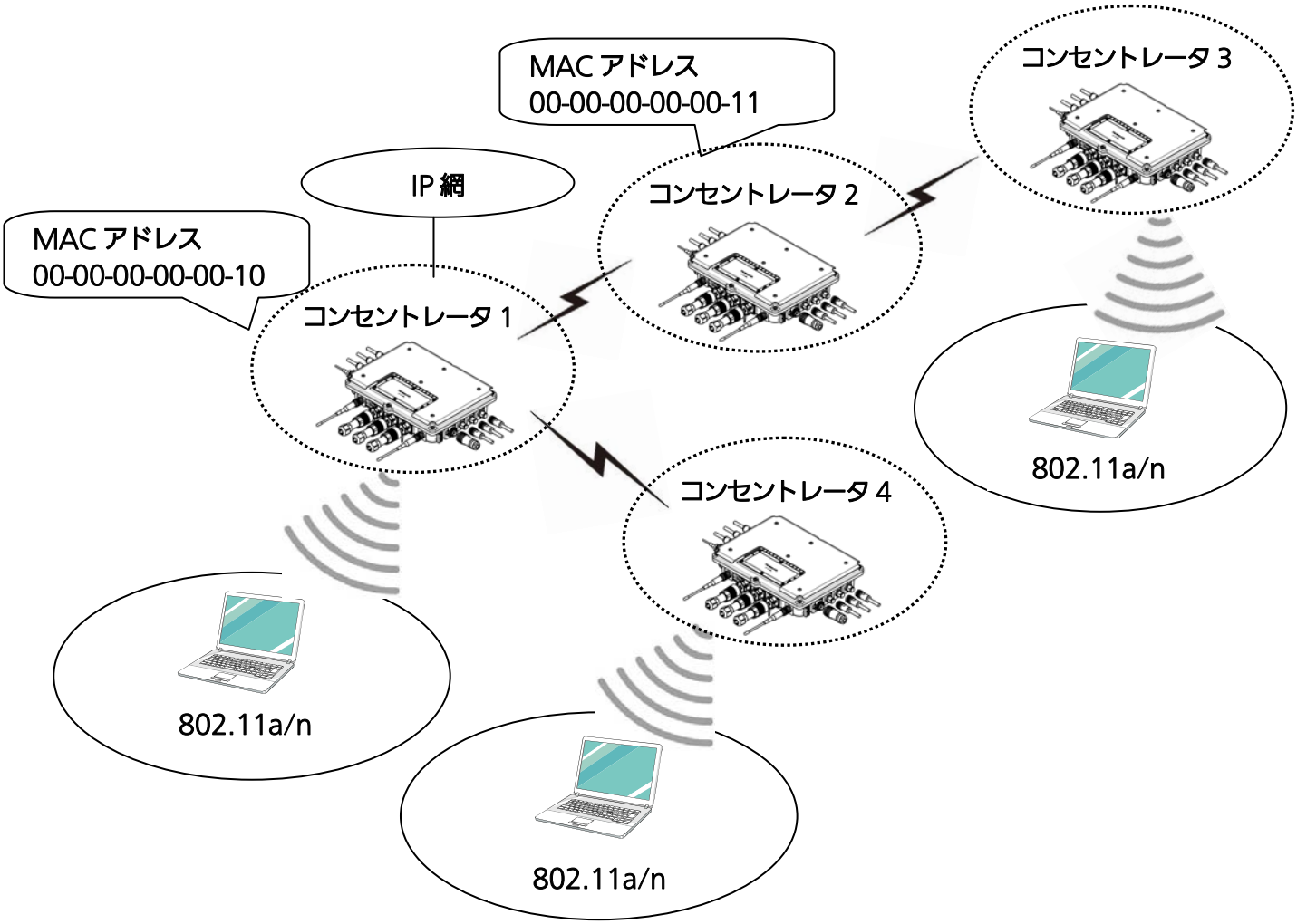


図4.5-1　　構成例（無線ブリッジ）

重要	■ 多段接続になった場合、サーバ側コンセントレータに各クライアント側コンセントレータの通信が集約されるので、スループットを考慮してネットワークを構築してください。 ■ クライアント側コンセントレータのチャネル制御が〔固定〕の場合は、サーバ側コンセントレータ のチャネルに合わせてください。クライアント側コンセントレータでチャネル制御が自動の場合は、チャネル設定不要です。 ■ 無線ブリッジを行っている状態で端末を収容するには、「端末接続許可設定」を〔許可〕にする必要があります。

設定手順

◆サーバ側コンセントレータ（コンセントレータ 1）の設定

ここではインターフェース（IF1）設定を例に説明します。インターフェース（IF2）設定選択時の設定方法も同様です。

手順1　〔Wi-Fi〕　→　〔無線管理〕　→　〔インターフェース（IF1）設定〕を選択します。

図4.5-2　メニュー（インターフェース(IF1)設定）

手順2　〔無線ブリッジ〕をクリックします。

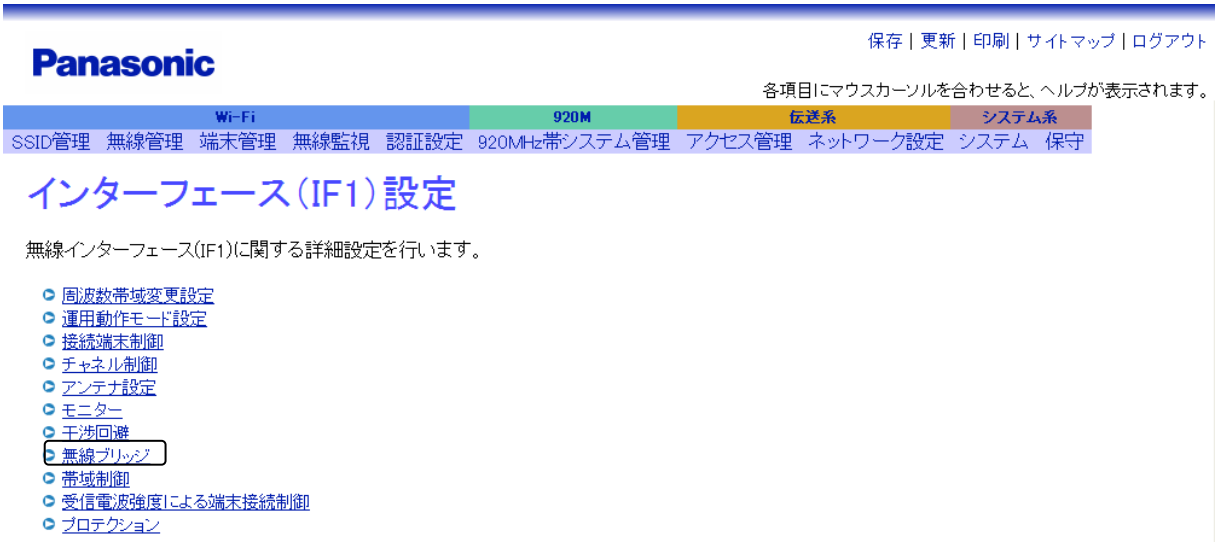


図4.5-3　インターフェース（IF1）設定

手順3　無線ブリッジの設定を行います。

- 端末接続許可設定の〔許可〕を選択
- 無線ブリッジ動作許可設定の〔有効〕を選択

※無線ブリッジ動作許可設定の設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

図4.5-4　無線ブリッジ

手順4　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

◆サーバ兼クライアント コンセントレータ（コンセントレータ 2）の設定

コンセントレータ 2 に対しては、サーバ設定 とクライアント設定 の両方が必要となります。
はじめに、上記 ◆サーバ側コンセントレータ（コンセントレータ 1）の設定 を行い、続いて以下の手順 5 ～ 手順 8 を行います。

手順5　〔無線管理〕　→　〔無線ブリッジ共通設定〕を選択します。

図4.5-5　メニュー（無線ブリッジ共通設定）

手順6　〔無線ブリッジ共通設定〕をクリックします。

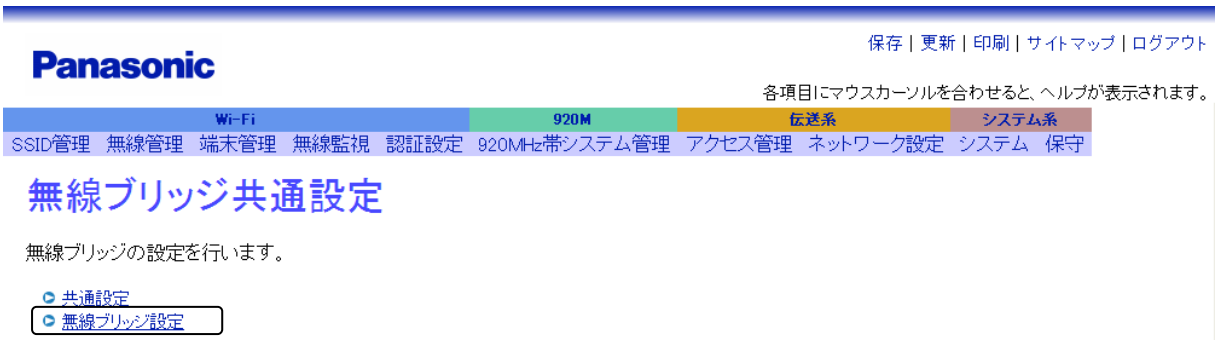


図4.5-6　無線ブリッジ共通設定

手順7　無線ブリッジ共通設定を行います。

- 無線ブリッジクライアント動作設定の〔IF1〕を選択
- 無線ブリッジ事前登録サーバ AP 設定に、コンセントレータ 1 の MAC アドレス「00-00-00-00-00-10」を入力
  （サーバ AP を特定しない場合は、本設定は不要です。）

これらの設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

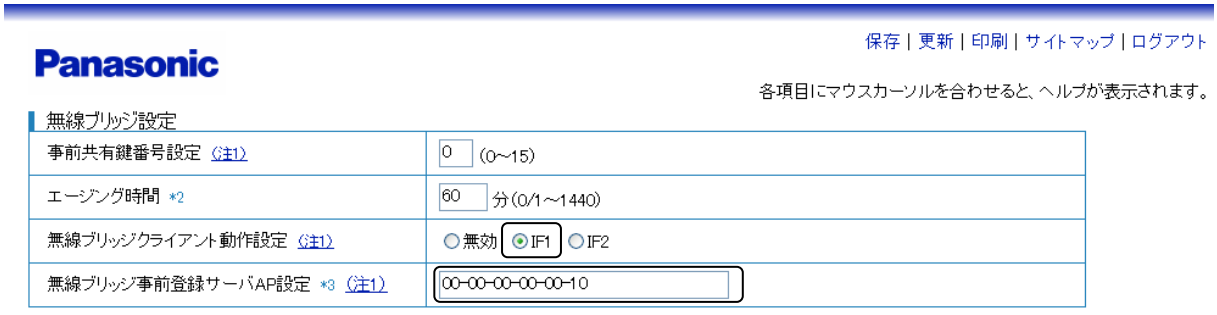


図4.5-7　無線ブリッジ共通設定

手順8　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

◆ クライアント側コンセントレータ（コンセントレータ 3）の設定
コンセントレータ 3 に対しては、クライアント設定のみが必要となります。

手順9　〔無線管理〕　→　〔インターフェース（IF1）設定〕、または〔インターフェース（IF2）設定〕を選択します。（図 4.5-2）
手順10　〔無線ブリッジ〕をクリックします。（図 4.5-3）
手順11　無線ブリッジの設定を行います。
・ 端末接続許可設定の〔許可〕を選択
・ 無線ブリッジ動作許可設定の〔無効〕を選択
※クライアント側コンセントレータ（コンセントレータ 3）では、サーバ AP 設定は不要なため、無線ブリッジ動作許可設定を〔無効〕に設定します。

図4.5-8　無線ブリッジ

手順12　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

引き続き ◆サーバ兼クライアント コンセントレータ（コンセントレータ 2）の設定 の手順 5 ～ 手順 8 を行います。
コンセントレータ 3 のサーバ側コンセントレータはコンセントレータ 2 となるため、手順 7 にて入力する MAC アドレスはコンセントレータ 2 の MAC アドレス「00-00-00-00-00-11」となります。

◆ クライアント側コンセントレータ（コンセントレータ 4）の設定
コンセントレータ 4 に対しては、クライアント設定のみが必要となります。
◆サーバ兼クライアント コンセントレータ(コンセントレータ 3)の設定 の手順 9 ～ 手順 12 を行います。
引き続き◆サーバ兼クライアント コンセントレータ（コンセントレータ 2）の設定 の手順 5 ～ 手順 8 を行います。

以上で、コンセントレータ間無線ブリッジ機能の設定は完了です。

コンセントレータでは、下の図に示すような並列接続の設定をすることも可能です。

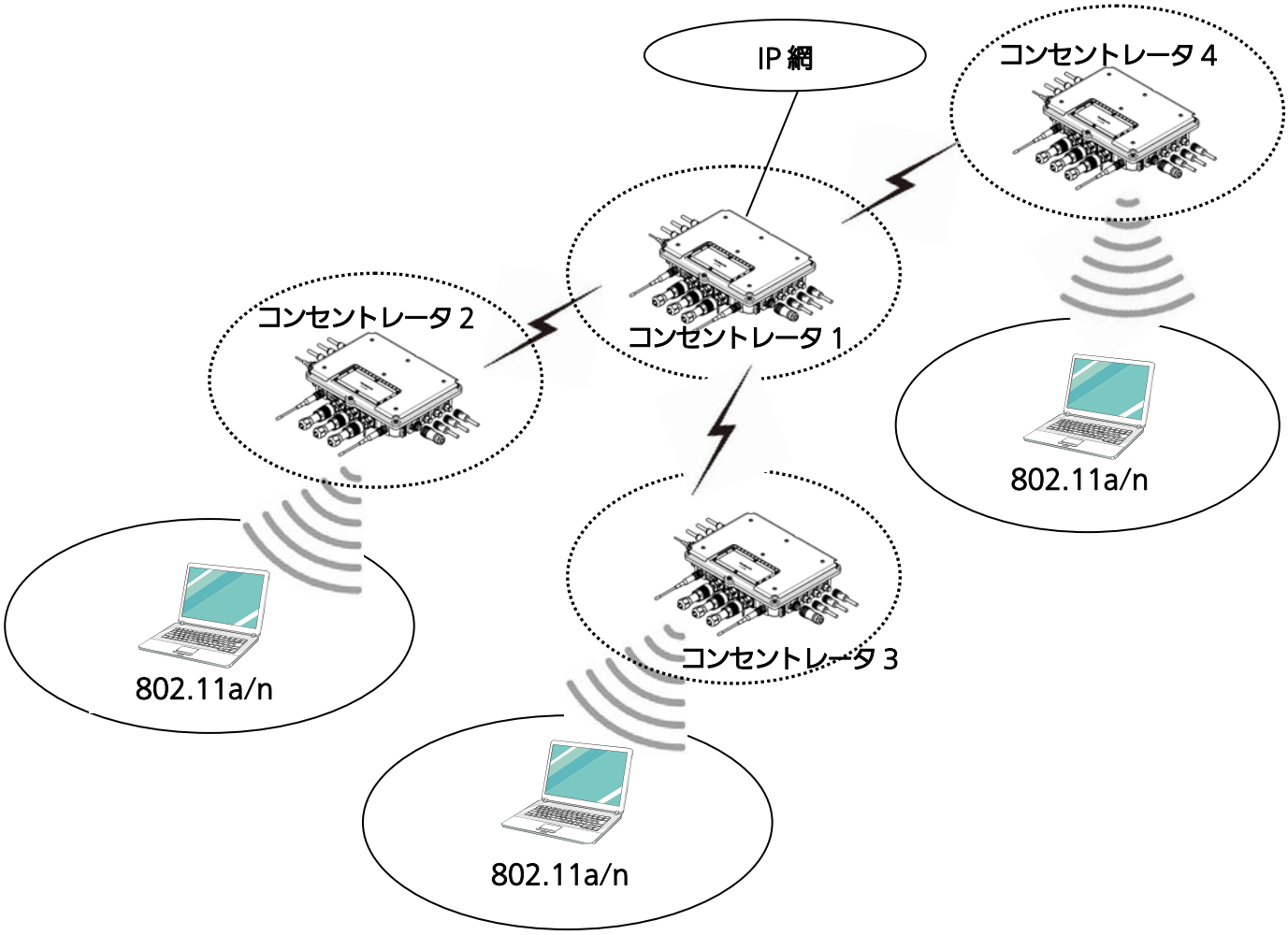


図4.5-9　構成例（無線ブリッジ）

4.6　VoIP 利用時の各種設定

コンセントレータには、VoIP 利用時の通話品質を維持するための機能が用意されています。ここでは、VoIP 利用時の各種設定方法を紹介します。

4.6.1　通話数制限機能

コンセントレータ には、3 種類の通話数制御機能（コール・アドミッション・コントロール、TSPEC、通信量）が用意されています。

■コール・アドミッション・コントロールによる端末接続数制御

コール・アドミッション・コントロール機能によって、端末接続数に応じて発呼／着呼制限や、非通話端末の切断など呼の管理を行うことも可能です。

コール・アドミッション・コントロール機能では、通信量ではなく、SIP のセッション制御を監視して、呼を管理します。この方式では、即時に通話中／非通話を判断できるため、より効率的な端末接続数制御が可能となります。

表4.6-1　通話数による端末数制御一覧表

閾値	説明
通話開始拒否	通話端末がこの閾値に達した場合、新規の通話は拒否されます。
新規端末拒否	通話端末がこの閾値に達した場合、新規の接続要求端末は拒否されます。
非通話端末切断	通話端末がこの閾値に達した場合、アイドル状態の端末は切断されます。

※コンセントレータを通過する SIP フレームが暗号化されていなかった場合のみ、監視が可能となります。

設定手順

手順1　〔Wi-Fi〕 → 〔端末管理〕 → 〔コール・アドミッション・コントロール〕 → 〔コール・アドミッション・コントロール設定〕を選択します。

図4.6-1　メニュー（コール・アドミッション・コントロール設定）

手順2　〔コール・アドミッション・コントロール有効／無効〕をクリックします。

図4.6-2　コール・アドミッション・コントロール設定

手順3　コール・アドミッション・コントロールを〔有効〕にします。

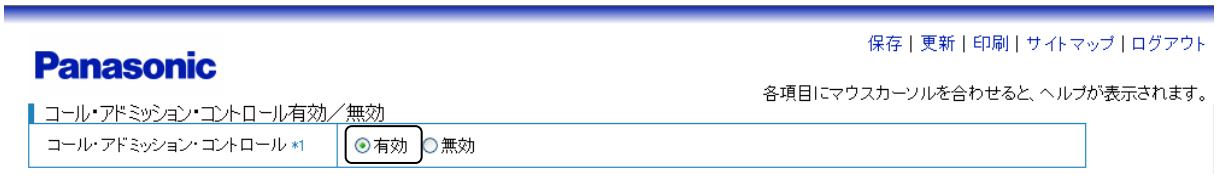


図4.6-3　コール・アドミッション・コントロール有効／無効

手順4　不要なセッション情報と判断するまでのエージング時間を設定します。

例として、「20 秒」を設定します。

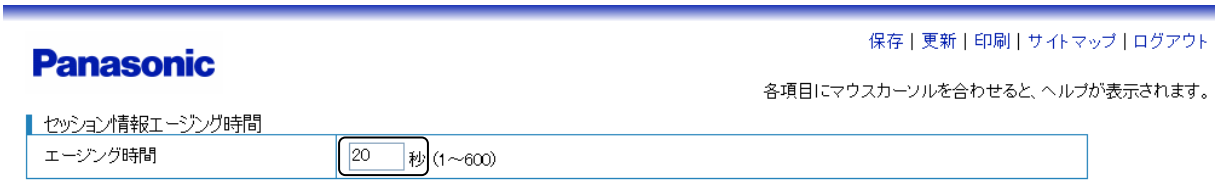


図4.6-4　セッション情報エージング時間

手順5　3 種類の通話接続制限の方法ごとの閾値を設定することで、コントロールの方法を指定します。

例として、2.4GHz 帯に下記設定を行います。

- 新規通話を拒否する閾値として、「200 台」
- 新規接続要求を拒否する閾値として、「215 台」
- アイドル状態の端末を切断する閾値として、「230 台」

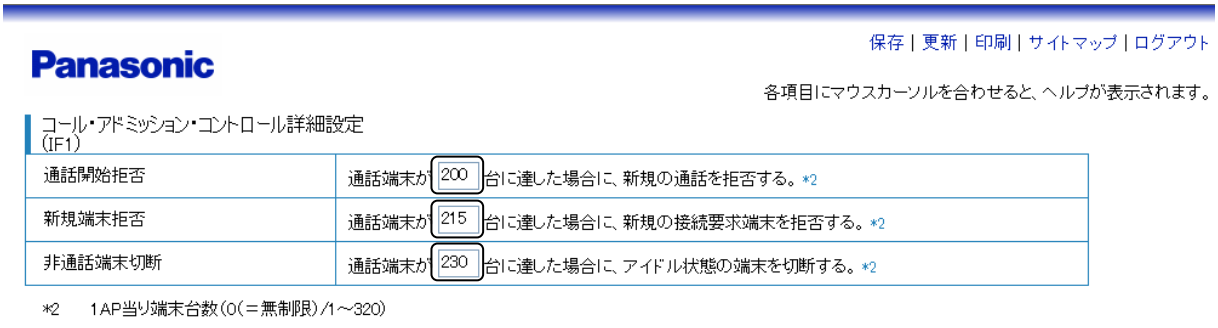


図4.6-5　コール・アドミッション・コントロール詳細設定（2.4GHz 帯）

手順6　新規の通話拒否を設定している場合は、拒否の方法を指定します。

例として、下記内容での設定を示します。

- 発呼制限方法として、〔通話拒否〕を選択
- 着呼制限方法として、〔端末切断〕を選択

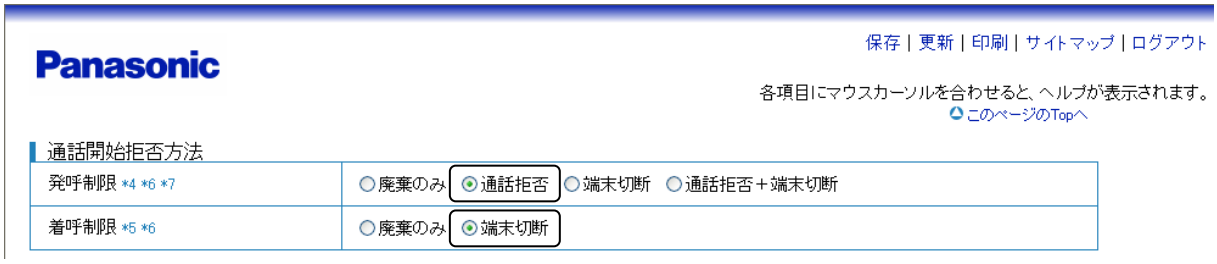


図4.6-6　通話開始拒否方法

手順7　画面最下部の〔設定〕をクリックし、設定を反映させます。

■TSPEC による通話数制御の設定

TSPEC とは、AC_VO（音声）、AC_VI（映像）に対する無線区間の品質確保を目的としたアドミッション制御機能です。TSPEC では、送信したいトラフィックの伝送条件をあらかじめマルチアクセス コンセントレータに伝え、利用可能な帯域を予約することで、通信品質を確保します。TSPEC 対応端末をご利用になる場合は、この機能を有効にすることをおすすめします。

設定手順

手順1　〔Wi-Fi〕 → 〔SSID 管理〕 → 〔SSID 設定〕を選択します。

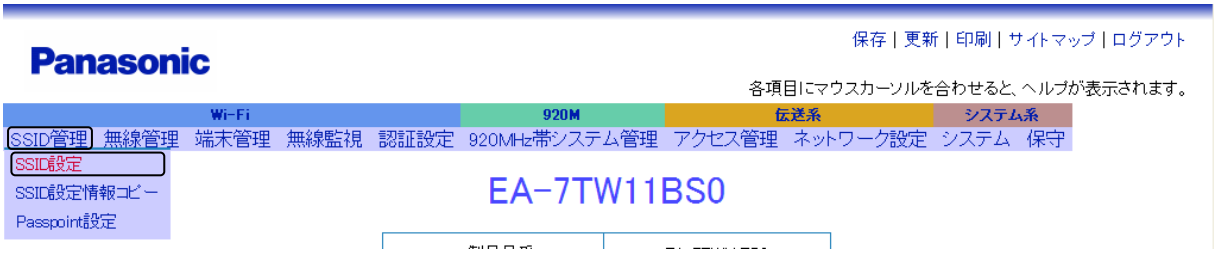


図4.6-7　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

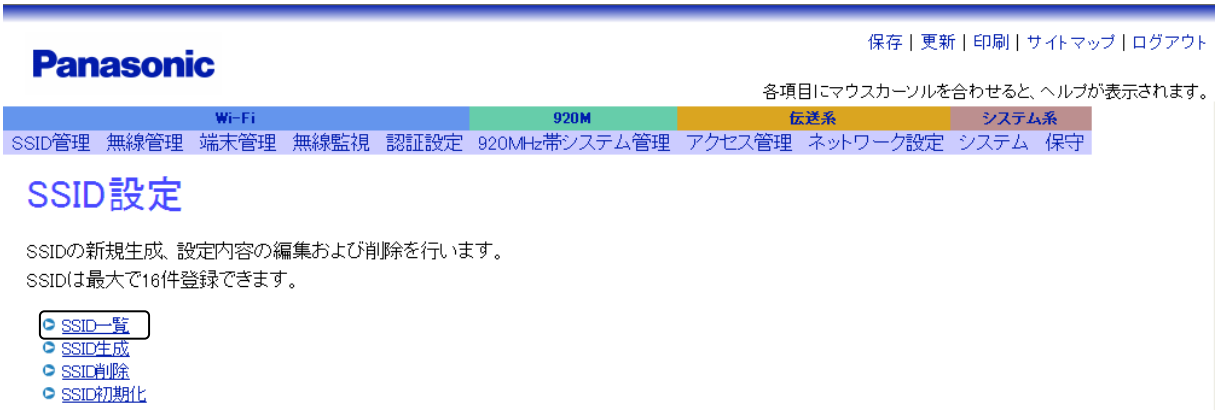


図4.6-8　SSID 設定

手順3　対象となる SSID の〔編集〕をクリックします。

図4.6-9　SSID 一覧

手順4　〔QoS〕をクリックします。

図4.6-10　SSID 編集

手順5　TSPEC に関するパラメーターを設定します。

例として、下記内容での設定を示します。

- 当該 SSID を〔WMM 規格に沿った QoS 制御〕に設定
- TSPEC アドミッション受付の音声と映像の両方を〔有効〕に設定

図4.6-11　QoS

手順6　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

■通信量による端末接続制御

通信量による端末接続制御機能では、端末単位に通信量（伝送パケット数）を監視し、通信量が閾値を上回る場合に通信中であるとみなし、通信端末数に基づいた接続制限を行います。

表4.6-2　通信端末数による通信数制御一覧表

閾値	説明
接続最大端末数	通信端末数がこの閾値に達した場合、新たな接続要求端末をすべて拒否します。
非通信端末切断	通信端末数がこの閾値に達した場合、アイドル状態のすべての端末を切断します。
通信端末切断	通信端末数がこの閾値に達した場合、通信中の端末を含めすべての端末を切断します。

ここでは、VoIP 端末の接続を優先したい場合の設定方法を紹介します。データ端末用の SSID（DATA）に対して、次のような設定を行います。

- 通信端末が 18 台に達した場合に、新たな接続要求端末を拒否する。
- 通信端末が 20 台に達した場合に、アイドル状態の端末を切断する。
- 通信端末が 22 台に達した場合に、通信している全端末を切断する。

たとえば、VOICE と DATA を介した通信端末数が合わせて 18 台に達すると、DATA を介した新たな端末の接続は拒否されます。さらに、VOICE を介して新たな VoIP 端末 2 台が通信し、通信端末数が 20 台に達すると、DATA を介して接続している端末の中で、アイドル状態の端末が切断されます。最終的に、総端末数が 22 台に達すると、DATA を介して通信をしている全端末が切断されて、VOICE を介して接続しようとしている VoIP 端末に十分な帯域が確保されます。

設定手順

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

図4.6-12　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

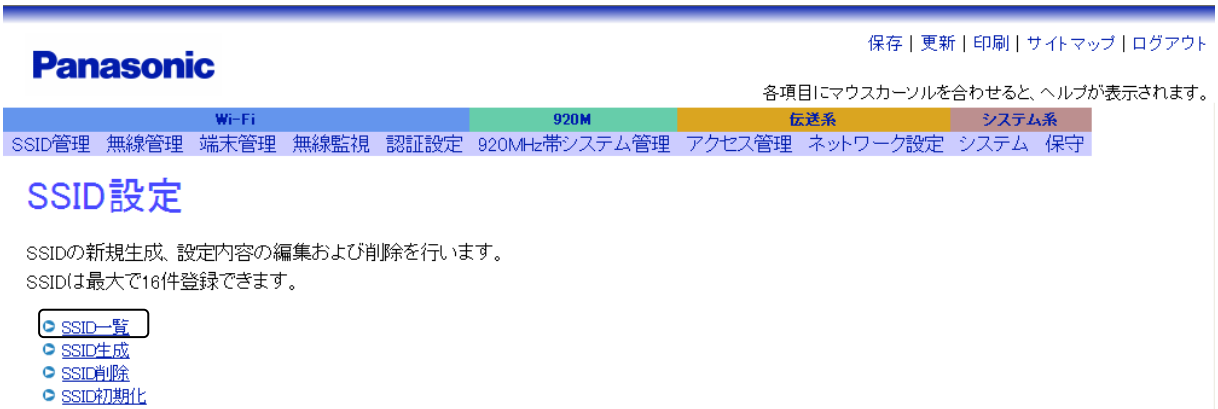


図4.6-13　SSID 設定

手順3　対象となる SSID の〔編集〕をクリックします。

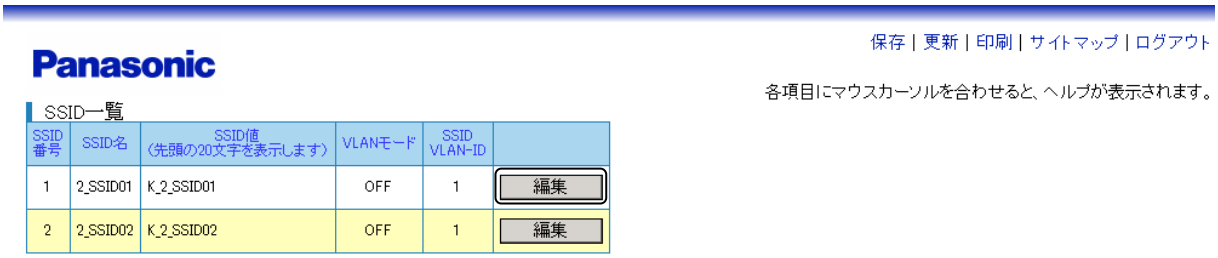


図4.6-14　SSID 一覧

手順4　通信端末数による端末接続制御をクリックします。

図4.6-15　SSID 編集

手順5　通信端末数による端末接続制御設定を行います。

例として、下記内容での設定を示します。

- 端末接続制御で〔使用する〕を選択
- 使用無線インターフェースは、〔IF1〕を選択
- 新規接続を拒否する閾値に「18 台」を設定
- アイドル状態の端末を切断する閾値に「20 台」を設定
- 通信中の全端末を切断する閾値に「22 台」を設定

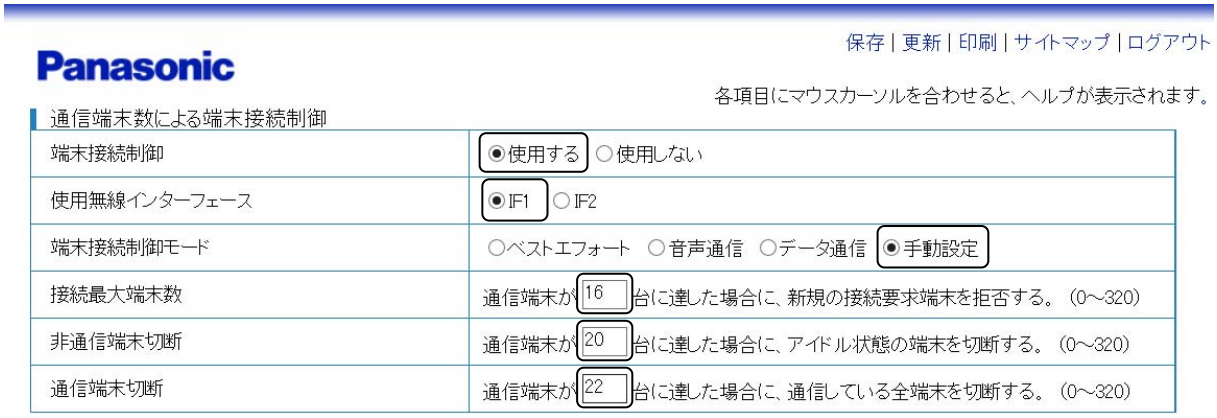


図4.6-16　通信中端末数による端末接続制御

手順6　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

4.6.2　代理 ARP 応答

コンセントレータは、端末の ARP 問い合わせに対して、代理 ARP を行うことができます。これによって省電力モードの端末が無駄に起動する必要がなくなるため、帯域と電力の両方を節約できます。
代理 ARP 応答動作には、未学習端末宛てフレーム透過と未学習端末宛てフレーム破棄の 2 種類があります。

未学習端末宛てフレーム破棄にすると、マルチアクセス コンセントレータで ARP テーブルに登録がない IP アドレスへの ARP 要求（無線 LAN 端末ではない装置への ARP 要求）を遮断するため、不要なフレームを無線上に送信せず、無線 LAN 端末の電力をより節約することができます。
ただし、この場合、無線 LAN 端末宛ての未学習 IP の ARP 要求はすべて遮断されるので、無線 LAN 端末やネットワーク内のほかの装置の ARP テーブルエージングタイマーを長く設定するなどして、マルチアクセス コンセントレータで学習した無線 LAN 端末の ARP テーブルがエージングされる前に更新されるように、運用してください。
コンセントレータの代理 ARP 応答は IPv4/v6 の両方に対応しており、下記で説明する設定は IPv4/v6 で共通です。

設定手順

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

図4.6-17　SSID 設定

手順2　〔SSID 一覧〕をクリックします。

図4.6-18　SSID 設定

手順3　対象となる SSID の〔編集〕をクリックします。

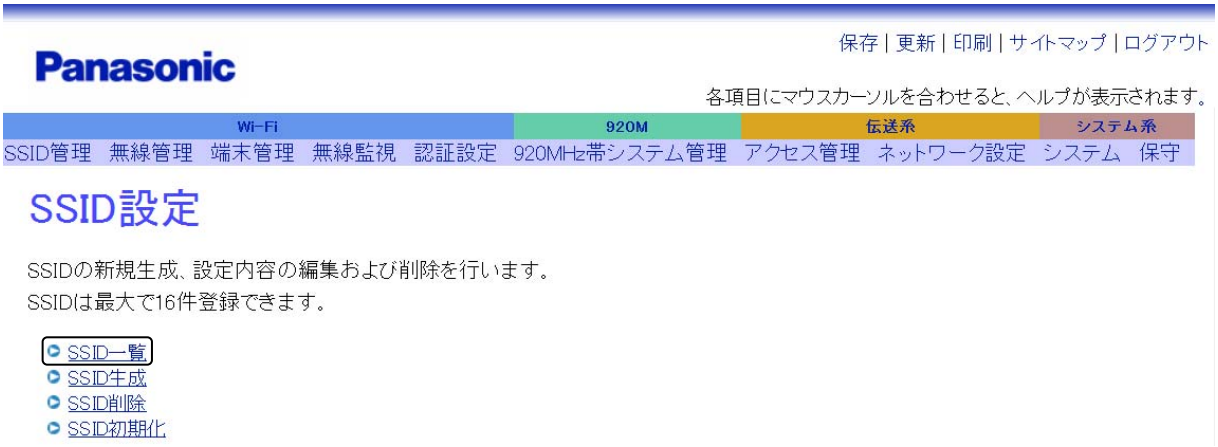


図4.6-19　SSID 一覧

手順4　〔代理 ARP 応答〕をクリックします。

図4.6-20　SSID 編集

手順5　代理 ARP 応答動作を設定します。

例として、下記内容での設定を示します。

- 代理 ARP 応答動作を〔未学習端末宛てフレーム破棄〕に設定
- 代理応答端末エージングタイマーを「3600 秒」に設定

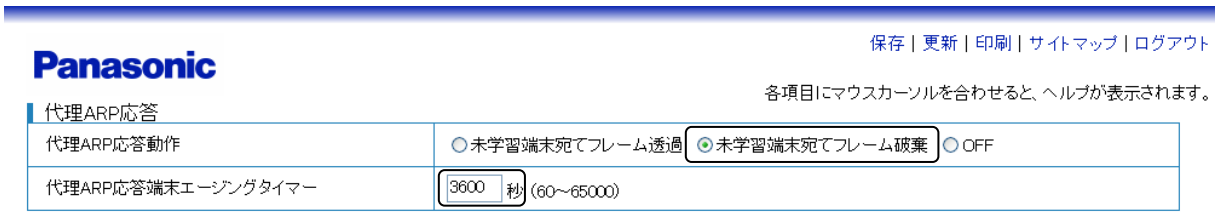


図4.6-21　代理 ARP 応答

手順6　画面最下部の〔設定〕をクリックし、設定を反映させます。

4.6.3　VoIP/Video 自動優先割り当て

SIP パケットのスヌーピングを行い、VoIP、および Video データの優先度を自動的に割り当てます。

設定手順

手順1　〔アクセス管理〕　→　〔QoS 設定〕を選択します。

図4.6-22　メニュー（QoS 設定）

手順2　〔音声フレーム優先制御設定〕をクリックします。

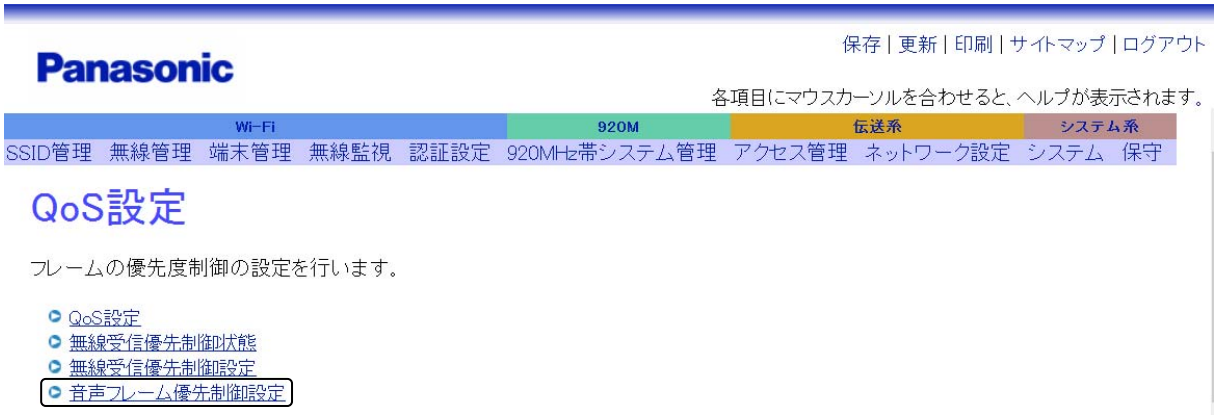


図4.6-23　QoS 設定

手順3　音声フレーム優先制御を〔有効〕にします。

図4.6-24　優先度自動設定

手順4　画面最下部〔設定〕をクリックし、設定を反映させます。

4.7　サービス品質向上機能

4.7.1　5GHz 帯への端末誘導設定

2.4GHz 帯は多くの機器が利用しており、無線帯域が混雑しているため、コンセントレータでは、5GHz 帯に対応している端末に対しては 2.4GHz 帯での接続を行わず、5GHz 帯での接続を促す機能を持ちます。
また、当機能は SSID 単位で設定が行えます。

設定手順

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

図4.7-1　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

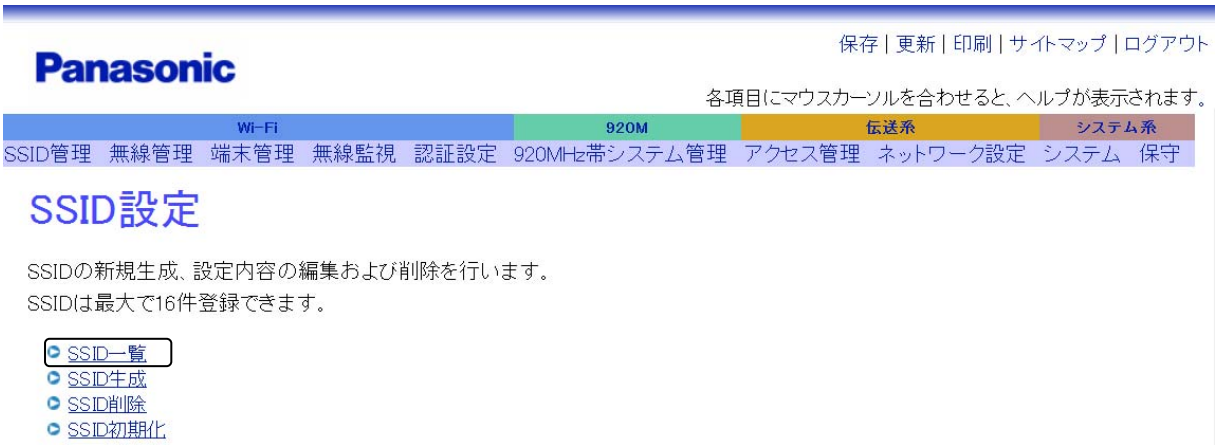


図4.7-2　SSID 設定

手順3　対象となる SSID の〔編集〕をクリックします。

図4.7-3　SSID 一覧

手順4　〔基本設定〕をクリックします。

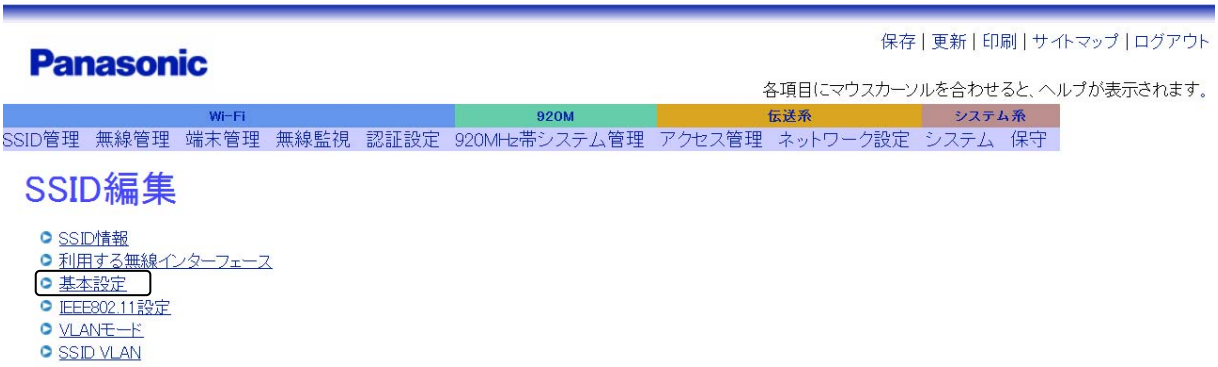


図4.7-4　SSID 編集

手順5　5GHz 帯への端末誘導 を〔有効〕にします。

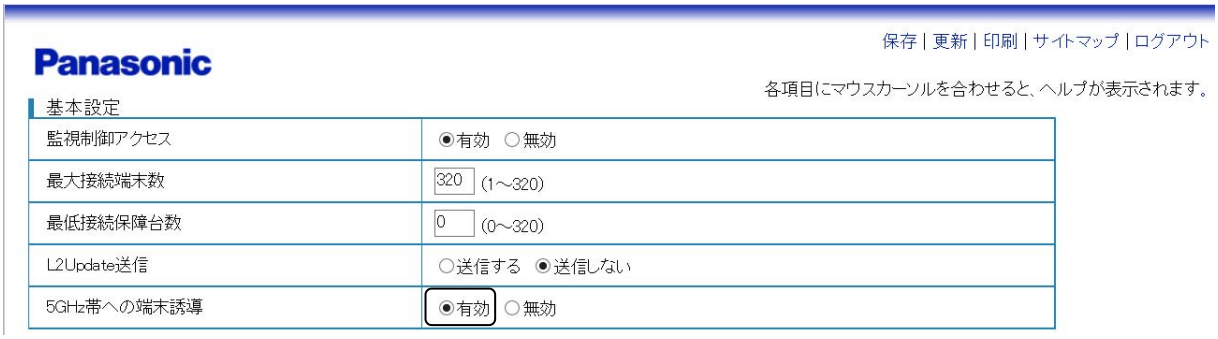


図4.7-5　基本設定

手順6　画面最下部の〔設定〕をクリックし、設定を反映させます。

4.7.2　小セル化（ビーコンレートの指定）

ビーコンの送信レートを上げることで、ビーコン検出可能エリアを安定した通信ができるエリアに絞り込み、電界が不安定なエリアの端末を接続させなくする（小セル化を実現する）ことで、通信サービスの品質を向上させます。

図4.7-6は、ビーコンレートを6Mbpsに指定することで、検出不可エリアの端末を接続させなくしています。

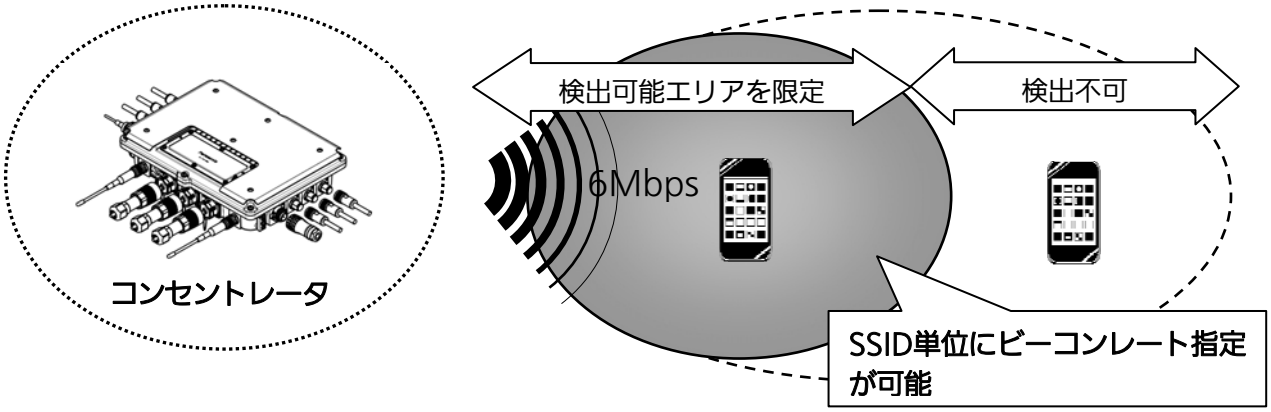


図4.7-6　ビーコンレート指定例

設定手順

手順1　〔無線管理〕　→　〔SSID 多重設定〕を選択します。

図4.7-7　メニュー（SSID 多重設定）

手順2　対象となる SSID の〔編集〕をクリックします。

例として、SSID：1 の編集を行います。

図4.7-8　SSID 多重設定

手順3　〔インターフェース（IF1）設定〕、または〔インターフェース（IF2）設定〕をクリックし、ビーコンレート制御の設定を行います。

例として、インターフェース（IF1）設定を選択し、設定を行います。

- ビーコンレート制御：〔有効〕を選択
- ビーコンレート：〔6M〕を選択

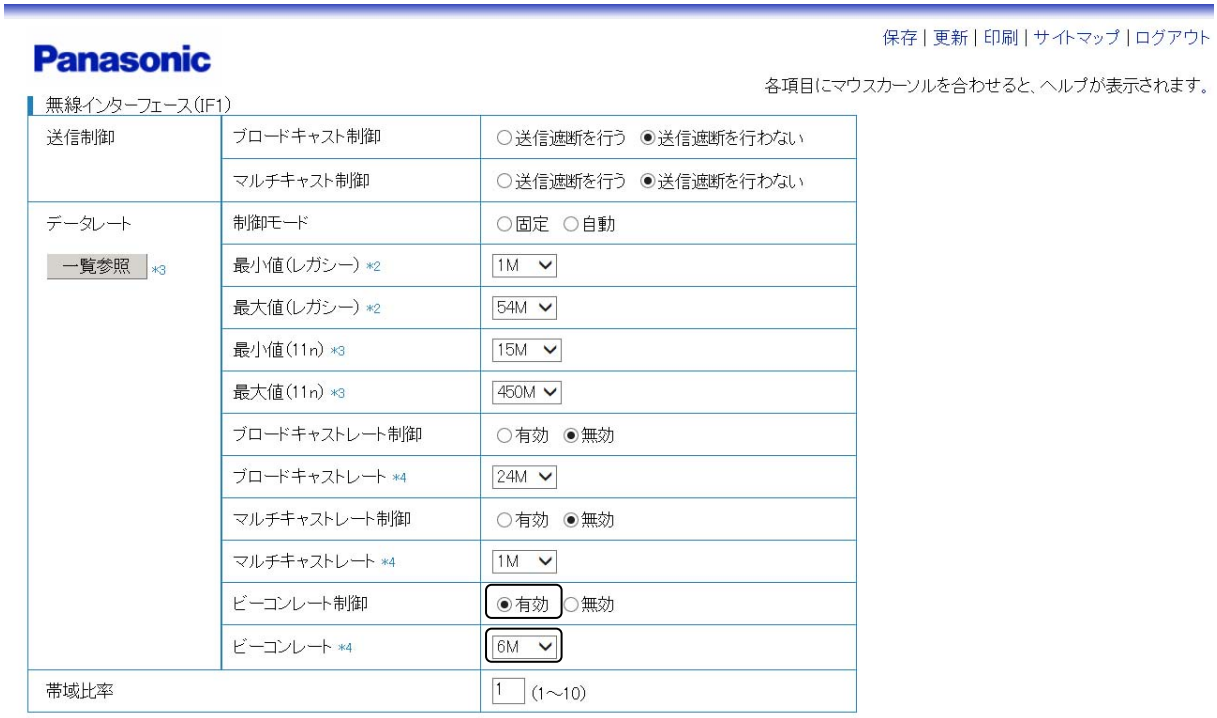


図4.7-9　インターフェース（IF1）設定（SSID 多重設定）

手順4　画面最下部の〔設定〕をクリックし、設定を反映させます。

4.7.3　同時接続端末数制御

マルチアクセス コンセントレータに、接続可能な最大端末数を設定することで、通信品質の極端な低下を回避できます。また、データ受信時に端末間の電界レベルを測定し、最大接続端末数に対する接続端末数の比率が設定した値に達した場合、一定の電界レベル（設定値）以下の端末からの接続を拒否することで、接続中の端末の通信品質を保つことも可能です。

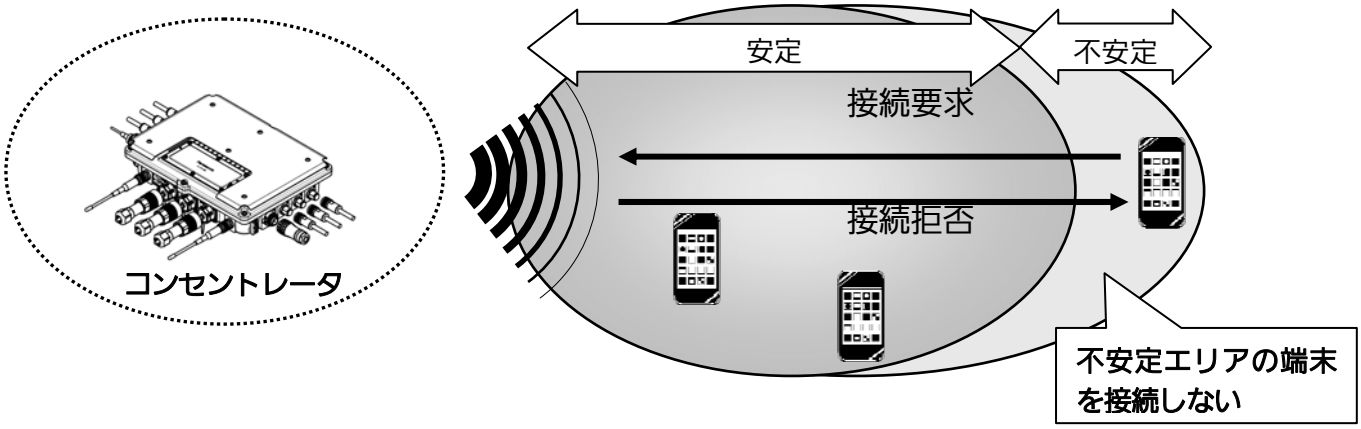


図4.7-10　受信電波強度による端末接続制御例

ここでは、インターフェース（IF1）設定を例に、最大接続数を固定で制限する方法と受信電波強度で端末接続数を制御する方法を紹介します。

設定手順

◆最大接続端末数設定

手順1　〔無線管理〕　→　〔インターフェース（IF1）設定〕を選択します。

図4.7-11　メニュー（インターフェース（IF1）設定）

手順2　〔接続端末制御〕をクリックします。

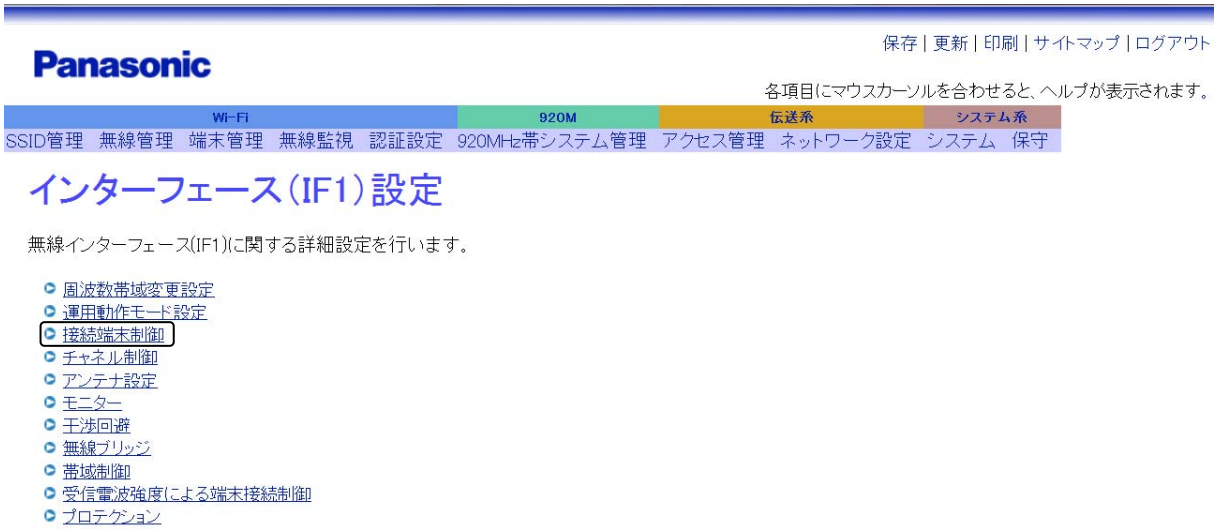


図4.7-12　インターフェース（IF1）設定

手順3　最大接続端末数を設定します。

※　この設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

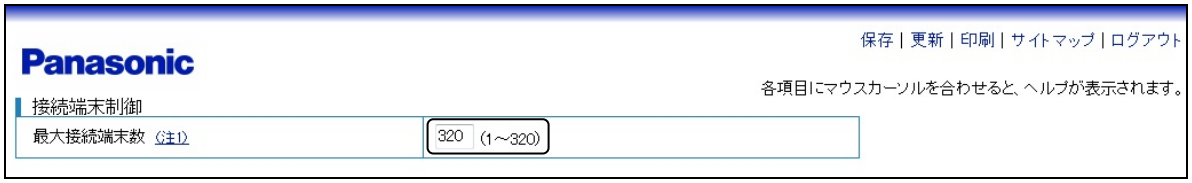


図4.7-13　接続端末制御

手順4　画面最下部〔設定〕をクリックし、設定を反映させます。

設定手順

◆受信電波強度による端末接続制御

手順1　〔Wi-Fi〕　→　〔無線管理〕　→　〔インターフェース（IF1）設定〕を選択します。

図4.7-14　メニュー（インターフェース（IF1）設定）

手順2　〔受信電波強度による端末接続制御〕をクリックします。

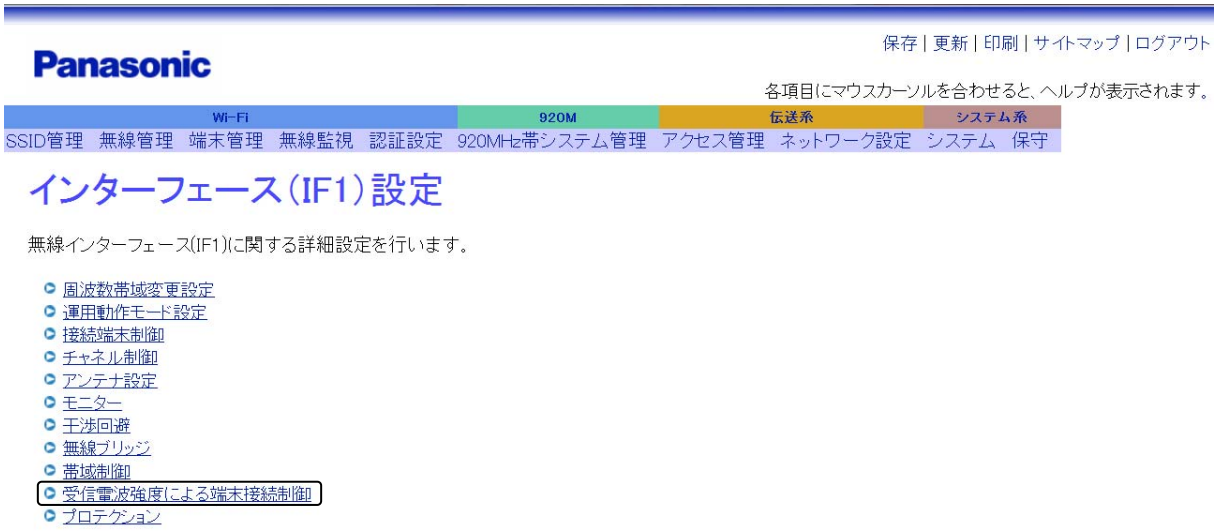


図4.7-15　インターフェース（IF1）設定

手順3　受信電波強度による端末接続制御の設定を行います。

例として、下記内容での設定を示します。

・　端末接続制御の〔有効〕を選択

・　端末接続制御の有効化割合に「80」を入力

上記設定では、最大接続端末数に対する接続端末数の比率が 80%以上となると、端末接続制御が動作します。

図4.7-16　受信電波強度による端末接続制御

手順4　画面最下部〔設定〕をクリックし、設定を反映させます。

4.7.4　最低接続保障台数制御

コンセントレータでは、最大接続端末数に加えて、最低接続保障台数を設定することができます。最低接続保障台数は SSID 単位で管理します。
各 SSID に対する最低接続保障台数の合計が無線インターフェースの最大接続端末数を超える場合、設定した台数分すべての端末接続が保障されなくなりますので注意してください。

例）使用する無線インターフェースの最大接続端末数：5 台
　　最低接続保障台数を SSID1：2 台、SSID2：3 台とし、接続中端末は SSID1、2 ともに 2 台とします。

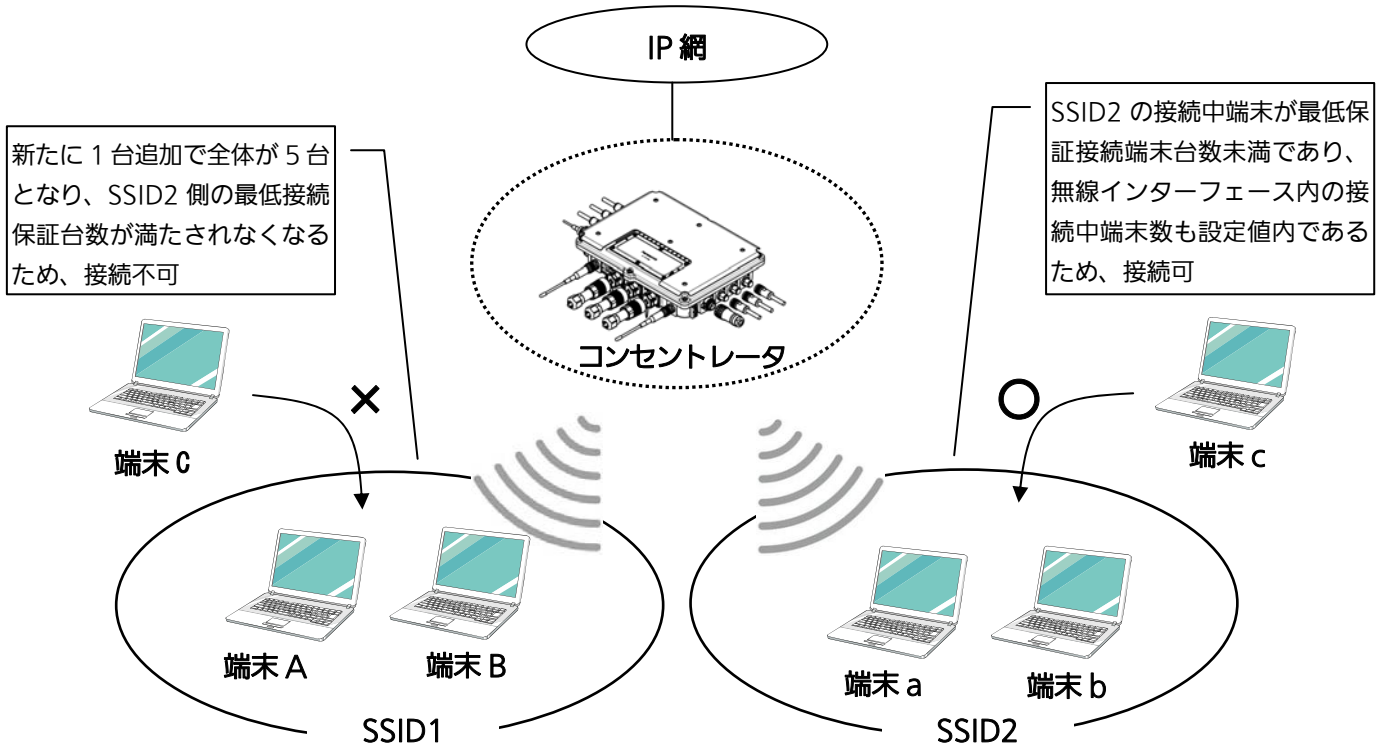


図4.7-17　　最低接続端末数制御例

設定手順

無線インターフェースの最大接続端末数は、前項 にて設定済みとして説明します。

手順1　〔Wi-Fi〕 → 〔SSID 管理〕 → 〔SSID 設定〕を選択します。

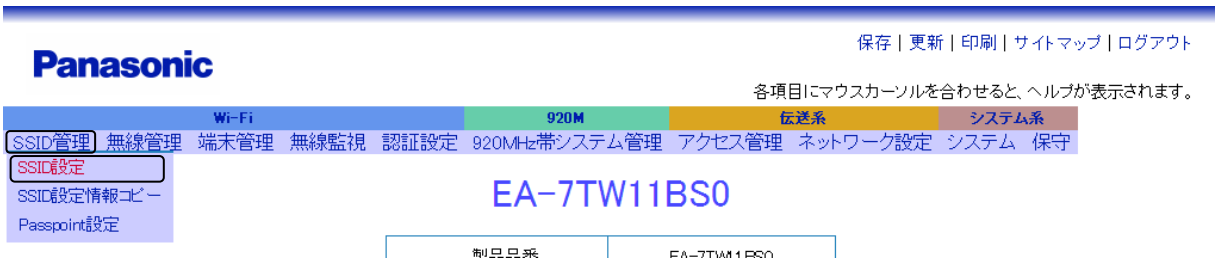


図4.7-18　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

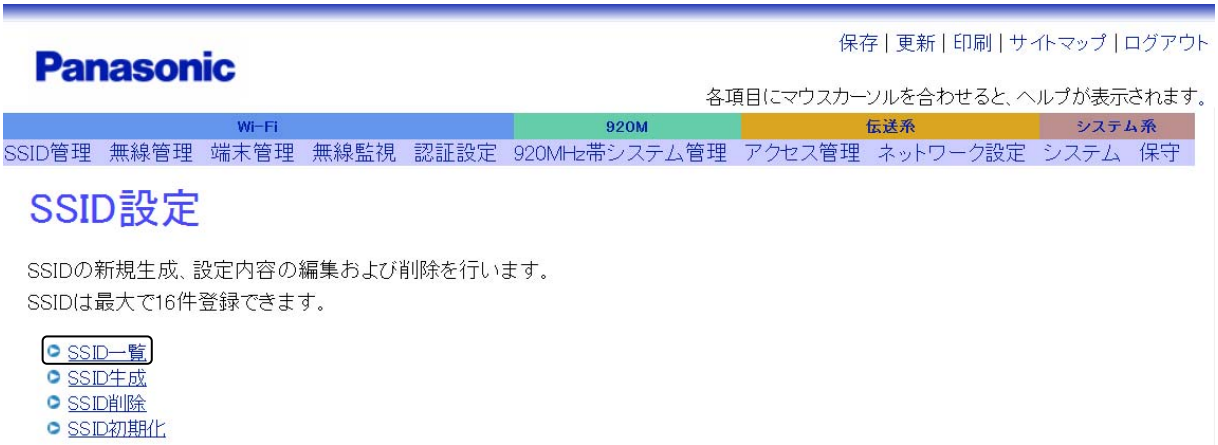


図4.7-19　SSID 設定

手順3　対象となる SSID の〔編集〕をクリックします。

例として、SSID1 の設定を行います。

図4.7-20　SSID 一覧

手順4　〔基本設定〕をクリックします。

図4.7-21　SSID 編集

手順5　最低接続保障台数に「2」を入力します。

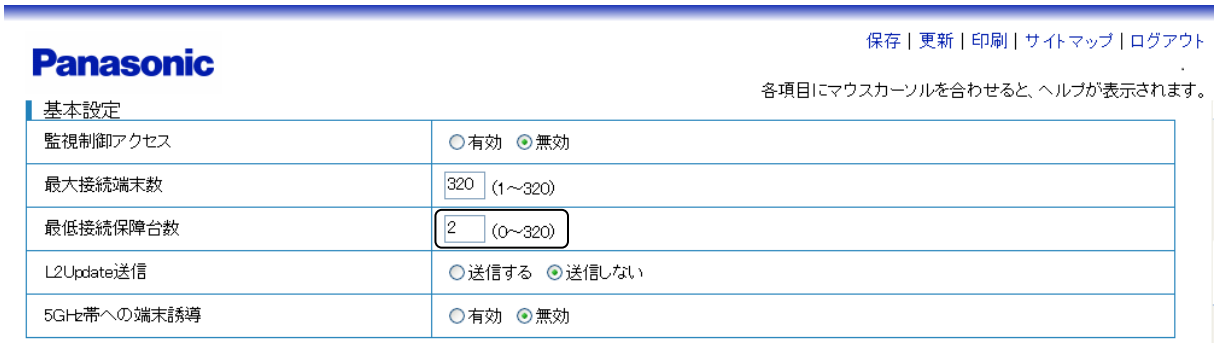


図4.7-22　最低接続保障台数

手順6　画面最下部の〔設定〕をクリックし、設定を反映させます。

4.7.5　IGMP スヌーピング

IGMP スヌーピング機能は、上位ルーターと端末間の IGMP トラフィックを覗き見（スヌーピング）し、マルチキャストが存在しない SSID に対するトラフィックを抑制することで、無駄なマルチキャストトラフィックを削減します。この機能によって、無線 LAN の通信品質が維持されます。
IGMP スヌーピング機能は、以下の 2 つの機能から構成されています。

- マルチキャストグループ管理機能
- マルチキャストフレームフィルタリング機能

IGMP スヌーピング機能を有効にすると、コンセントレータ は無線 LAN 端末から送信される IGMP トラフィック（Membership Report）で通知されるマルチキャストグループを学習し、各 SSID 配下に存在するマルチ
キャストグループの管理を開始します。
また、あるマルチキャストグループに属する SSID 配下の無線 LAN 端末から、そのグループに該当する Membership Report を一定時間受信しない場合、その SSID をグループから除外します。この時間をグループエージングタイマーと呼びます。
ここでは、IGMP スヌーピング機能を有効にするための方法を紹介します。

設定手順

手順1　〔Wi-Fi〕 → 〔SSID 管理〕 → 〔SSID 設定〕を選択します。

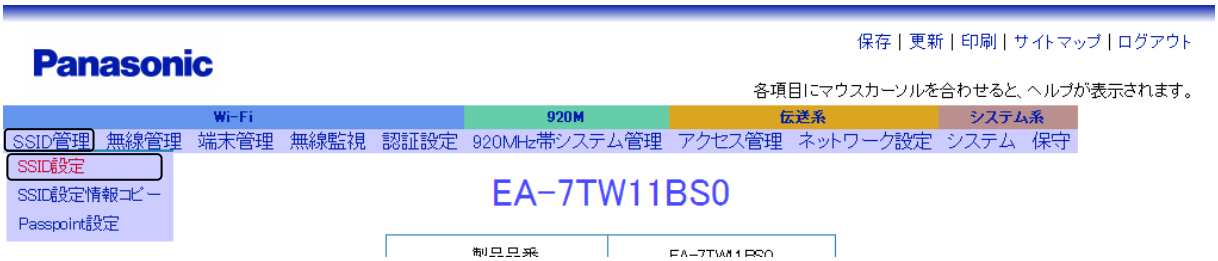


図4.7-23　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

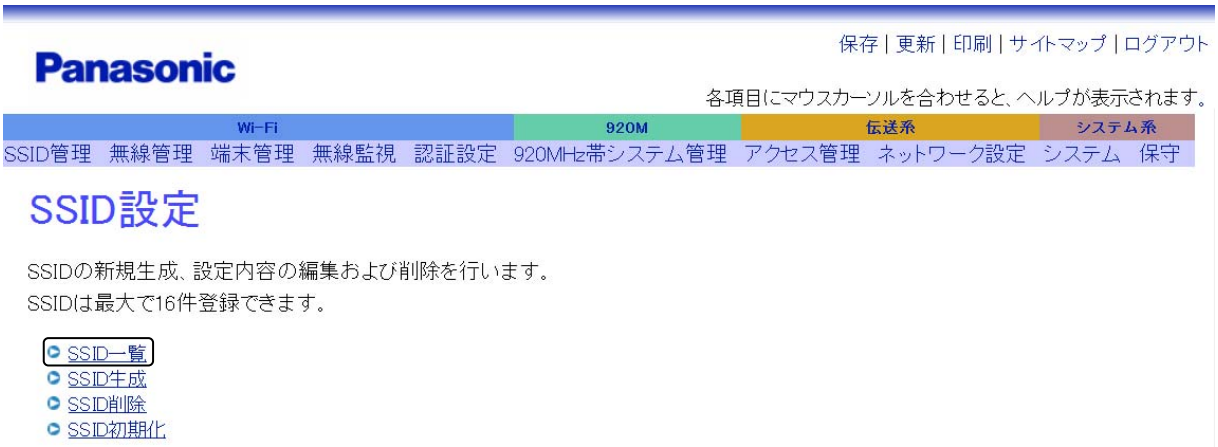


図4.7-24　SSID 設定

手順3　対象となる SSID の〔編集〕をクリックします。

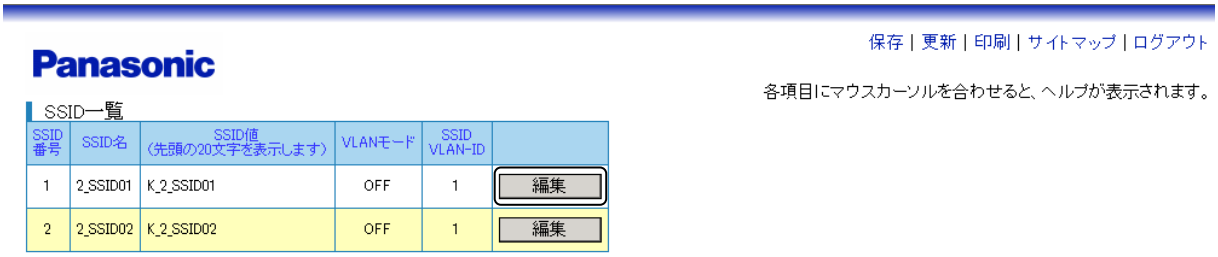


図4.7-25　SSID 一覧

手順4　〔IGMP スヌーピング〕をクリックします。

図4.7-26　SSID 編集

手順5　IGMP スヌーピングを〔有効〕にします。

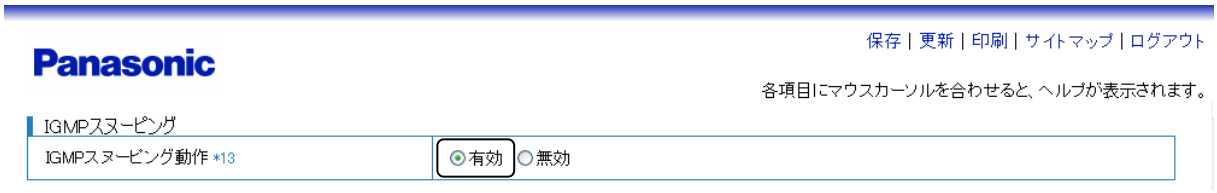


図4.7-27　IGMP スヌーピング

手順6　画面最下部の〔設定〕をクリックし、設定を反映させます。

※ グループエージングタイマー設定を行う場合は、下記をご参照ください。
〔アクセス管理〕　→　〔IGMP スヌーピング〕を選択します。

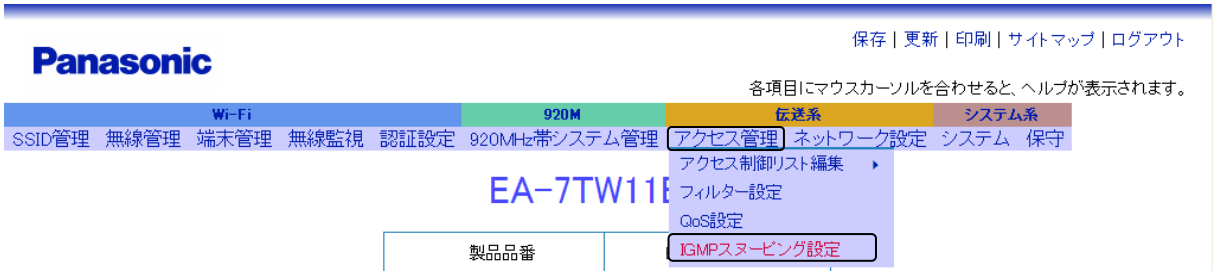


図4.7-28　メニュー（IGMP スヌーピング設定）

〔IGMP スヌーピング設定〕画面で、グループエージングタイマー設定します。
〔グループエージングタイマー〕は〔Query 間隔〕、〔Query 応答時間〕、〔Robustness 値〕を入力することで算出して表示されます。

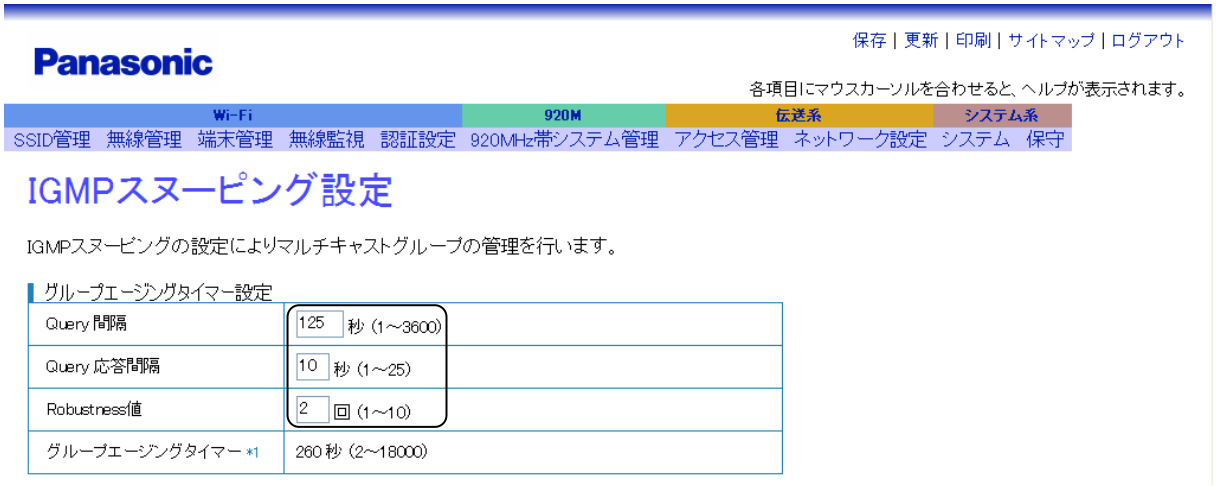


図4.7-29　IGMP スヌーピング設定（グループエージングタイマー設定）

手順7　画面最下部〔設定〕をクリックし、設定を反映させます。

■学習状況の確認

マルチキャストグループの学習状況に従って、マルチキャストフレームはフィルタリングされます。

たとえば、マルチキャストフレームの転送先 SSID の IGMP スヌーピング機能が有効の場合で、転送先 SSID に該当するマルチキャストグループが存在しなければ、そのフレームはフィルタリング機能によって不透過となります。ただし、同じマルチキャストアドレスの学習がほかに存在しない場合、そのフレームは転送されます。

マルチキャストグループの学習状況を確認にするための方法を紹介します。

操作手順

手順1　〔Wi-Fi〕 → 〔端末管理〕 → 〔マルチキャストグループ一覧〕を選択します。

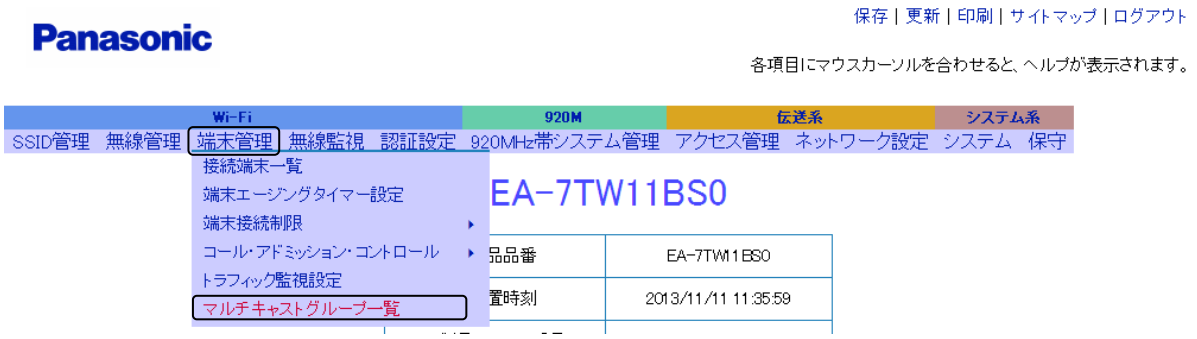


図4.7-30　メニュー（端末管理）

手順2　〔マルチキャストグループ一覧〕をクリックします。

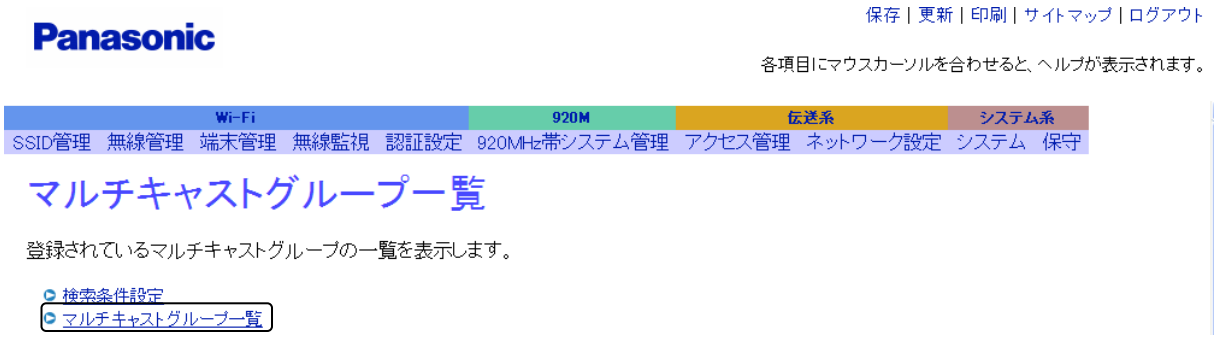


図4.7-31　マルチキャストグループ一覧

手順3　検索するマルチキャストグループの条件を入力します。

例として、下記内容での設定を示します。

・ IP アドレスに「224.1.1.1」を入力

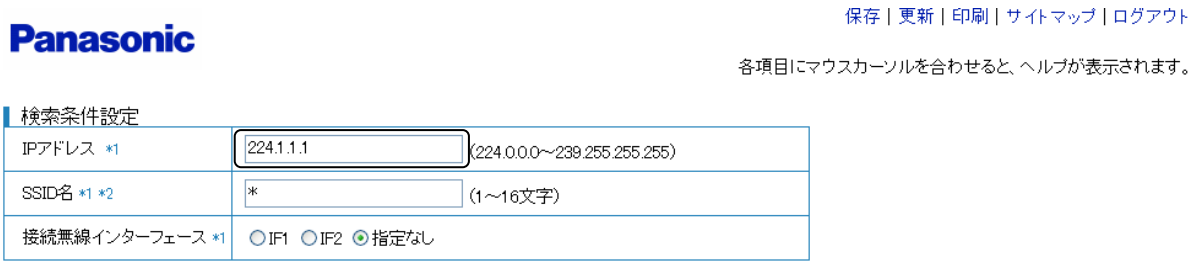


図4.7-32　マルチキャストグループ検索条件設定

手順4　〔設定〕をクリックし押すと、検索したマルチキャストグループ一覧を確認できます。

4.7.6　Passpoint 機能

Passpoint は、Wi-Fi Alliance によって策定された規格「Hotspot 2.0」のサービス名です。 コンセントレータの Passpoint は、以下の機能を提供します。（Wi-Fi Alliance フェーズ 1 に対応しています）

- ネットワークの発見および選択
  → ユーザが操作しなくても端末がネットワークを発見し、
  自動的に接続する機能を提供します。

- シームレスなネットワークアクセス
  → ブラウザでのサインオンや、ユーザによるパスワードの入力を必要とせず、
  SIM カードやユーザ名／パスワード、証明書に基づく EAP 認証を行うことにより
  シームレスなネットワークアクセスを提供します。

- 安全な認証および接続
  →セルラーネットワークに匹敵する安全性を提供します。

ここでは、Passpoint 機能を有効にするための方法を紹介します。

設定手順

手順1　〔Wi-Fi〕 →〔SSID 管理〕 → 〔Passpoint 設定〕を選択します。

図4.7-33　メニュー（Passpoint 設定）

手順2　対象となる SSID の〔編集〕をクリックします。

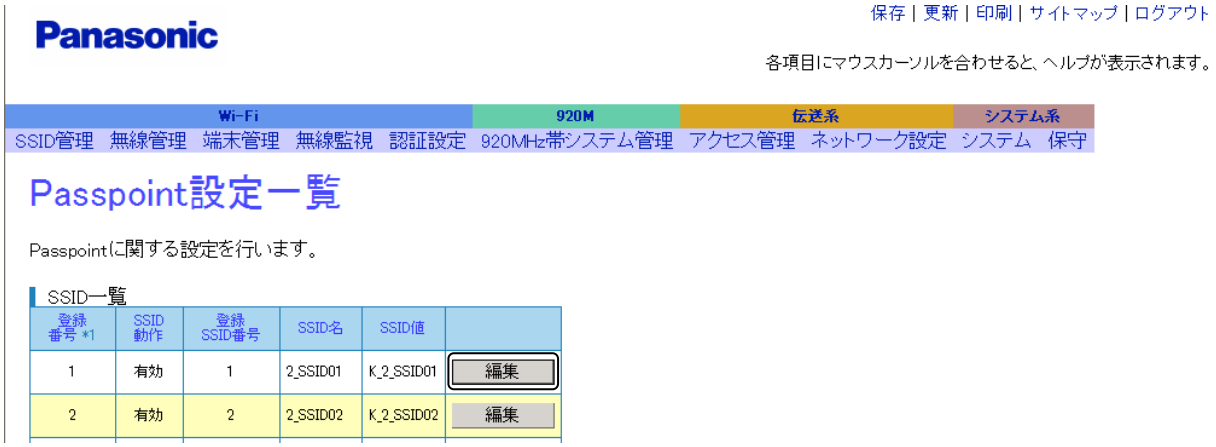


図4.7-34　Passpoint 設定一覧（SSID 一覧）

手順3　〔Passpoint 設定〕をクリックします。

図4.7-35　Passpoint 編集

手順4　Passpoint 設定を〔有効〕にします。

Passpoint 機能を、〔有効〕に機能させるためには、あらかじめ〔SSID 編集〕画面の〔セキュリティ（共通)〕項目にて WPA2 を〔有効〕、固定 WEP、動的 WEP、TKIP をそれぞれ〔無効〕に設定してください。

図4.7-36　Passpoint 設定

Passpoint 機能が〔有効〕の場合、コンセントレータから送信される Beacon フレームと Probe Response フレームに下記エレメントを付与します。各エレメントにフレキシブルな設定が可能です。ここでは各設定画面を紹介します。〔Passpoint 編集〕画面にて設定変更可能です。

表4.7-1　Beacon/Probe Response の付与エレメント一覧表

付与エレメント	各種設定
Interworking	＜設定変更可能＞ ・ネットワークタイプ設定 ・インターネット接続可否設定 ・HESSID 設定 ・Venue Group 設定 ・Venue Type 設定
Roaming Consortium	＜設定変更可能＞ ・ローミングコンソーシアム設定
BSS Load	＜設定変更不可＞ 端末接続台数やチャネル利用率などの状態値を付与します。
Advertisement Protocol	＜設定変更不可＞ 固定値を付与します。
P2P	＜設定変更不可＞ 固定値を付与します。
Hotspot 2.0 Indication	＜設定変更可能＞ ・DGAF 設定

◆ **Interworking エレメントに関する設定画面**

［Passpoint 編集］画面（図 4.7-35）の［アクセスネットワークタイプ設定］をクリックします。

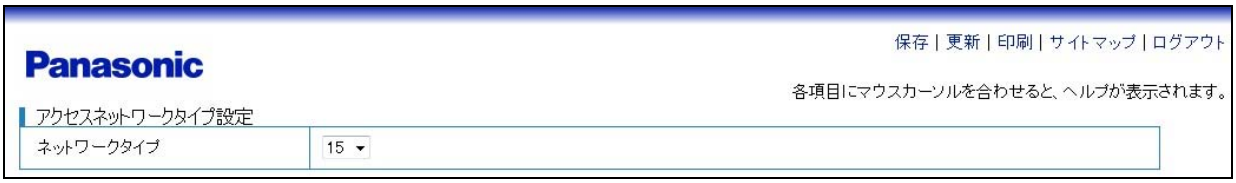


図4.7-37　アクセスネットワークタイプ設定

［Passpoint 編集］画面（図 4.7-35）の［インターネット接続可否設定］をクリックします。

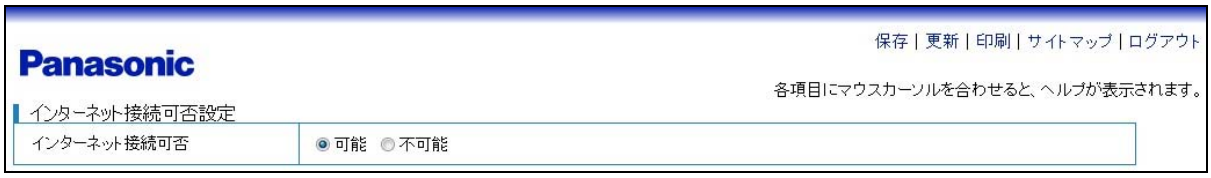


図4.7-38　インターネット接続可否設定

［Passpoint 編集］画面（図 4.7-35）の［HESSID 設定］をクリックします。

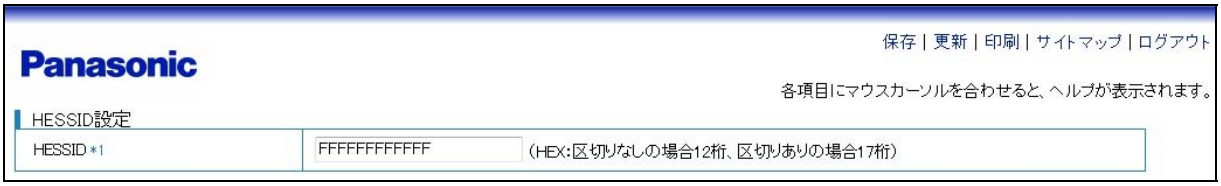


図4.7-39　HESSID 設定

［Passpoint 編集］画面（図 4.7-35）の［Venue Info 設定］をクリックします。

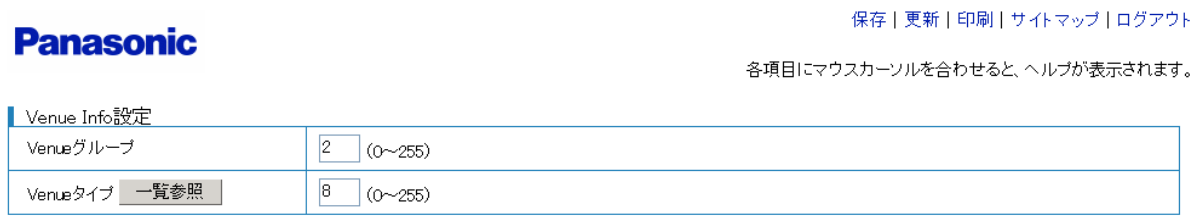


図4.7-40　Venue Info 設定

［Venue Info 設定］画面（図 4.7-40）の［一覧参照］をクリックします。

Venueタイプ一覧

Venueグループ		Venueタイプ	
番号 *1	詳細	番号 *1	詳細
0	未指定	0	未指定
1	集合場所	0	未指定
		1	アリーナ
		2	スタジアム
		3	ターミナル
		4	円形劇場
		5	遊園地
		6	礼拝所
		7	会議場
		8	図書館
		9	博物館
		10	レストラン
		11	映画館
		12	バー
		13	コーヒーショップ
		14	動物園または水族館
		15	緊急対応センター
2	ビジネス	0	未指定
		1	診療所または歯科医院
		2	銀行
		3	消防署
		4	警察署
		5	(予約)
		6	郵便局
		7	専門家事務所
		8	研究開発施設
		9	弁護士事務所
3	教育	0	未指定
		1	小学校
		2	中等学校
		3	大学
4	工業	0	未指定
		1	工場
5	施設	0	未指定
		1	病院
		2	介護施設
		3	アルコール＆薬物リハビリセンター
		4	グループホーム
		5	刑務所または留置所
6	商業	0	未指定
		1	小売店
		2	マーケット
		3	自動車サービスステーション
		4	ショッピングモール
		5	ガソリンスタンド
7	住居	0	未指定
		1	個人住居
		2	ホテルまたはモーテル
		3	寮
		4	下宿
8	倉庫	0	未指定
9	多目的	0	未指定
10	乗り物	0	未指定
		1	自動車またはトラック
		2	飛行機
		3	バス
		4	フェリー
		5	船またはボート
		6	列車
		7	バイク
11	屋外	0	未指定
		1	市営メッシュネットワーク
		2	都市公園
		3	休憩所
		4	交通管制
		5	バス停留所
		6	キオスク

*1　グループ、タイプのそれぞれの空いている番号(～255)は予約番号となります。

閉じる

図4.7-41　Venue タイプ一覧

◆ **Roaming Consortium エレメントに関する設定画面**

［Passpoint 編集］画面（図 4.7-35）の［ローミングコンソーシアム設定］をクリックします。

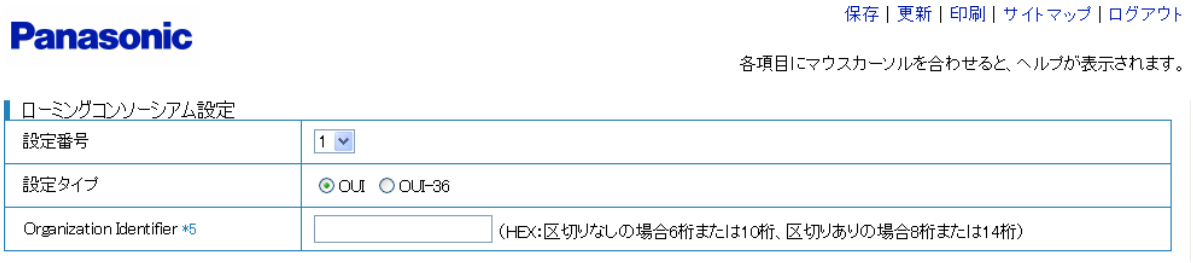


図4.7-42　ローミングコンソーシアム設定

Passpoint 機能の 1 つである「ネットワークの発見および選択」にあたり、コンセントレータでは端末からの GAS プロトコルを用いた問い合わせに対応しています。コンセントレータから送信される GAS Initial Response フレームに下記エレメントを付与します。各エレメントにフレキシブルな設定が可能です。ここでは各設定画面を紹介します。〔Passpoint 編集〕画面にて設定変更可能です。

表4.7-2　GAS Initial Response の付与エレメント一覧表

付与エレメント	各種設定
ANQP	＜設定変更可能＞ ・Venue Name 設定 ・ネットワーク認証種別設定 ・HTTP/HTTPS リダイレクション URL 設定 ・IPv4 アドレス利用可否設定 ・IPv6 アドレス利用可否設定 ・NAI Realm 設定 ・EAP メソッド設定 ・MCC 設定 ・MNC 設定 ・ドメイン名設定
Hotspot 2.0 ANQP	＜設定変更可能＞ ・オペレータフレンドリー名設定 ・リンク速度設定 ・コネクション状態設定

◆ **ANQP エレメントに関する設定画面**

［Passpoint 編集］画面（図 4.7-35）の［Venue Name 設定］をクリックします。

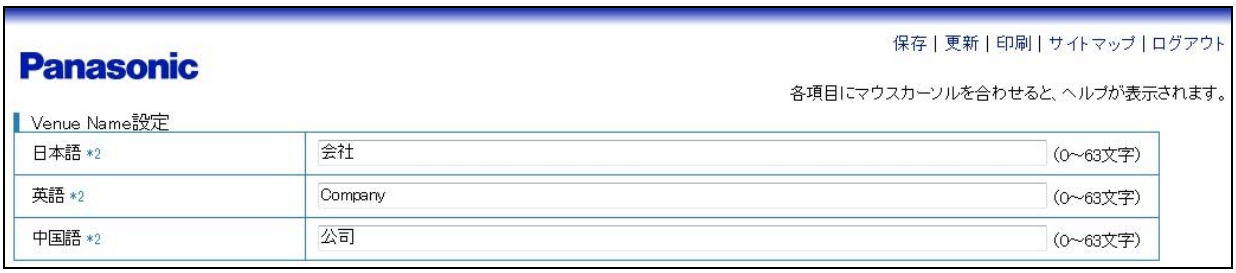


図4.7-43　Venue Name 設定

［Passpoint 編集］画面（図 4.7-35）の［ネットワーク認証種別設定］をクリックします。

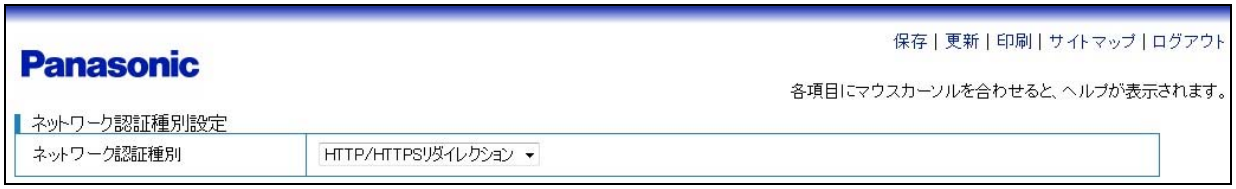


図4.7-44　ネットワーク認証種別設定

［Passpoint 編集］画面（図 4.7-35）の［HTTP/HTTPS リダイレクション URL 設定］をクリックします。

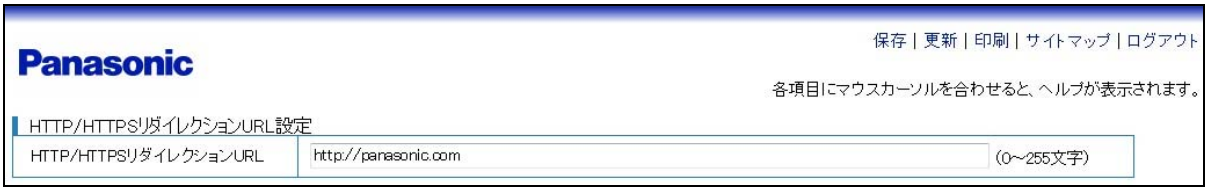


図4.7-45　HTTP/HTTPS リダイレクション URL 設定

［Passpoint 編集］画面（図 4.7-35）の［IPv4 アドレス利用可否設定］をクリックします。

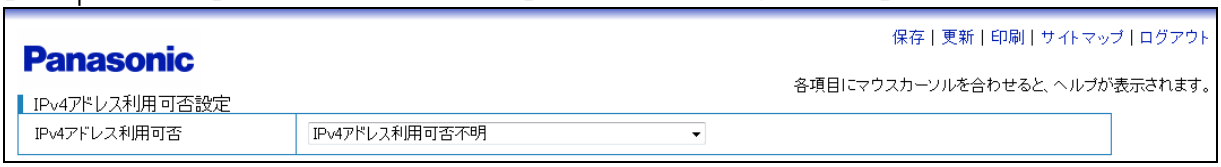


図4.7-46　IPv4 アドレス利用可否設定

［Passpoint 編集］画面（図 4.7-35）の［IPv6 アドレス利用可否設定］をクリックします。

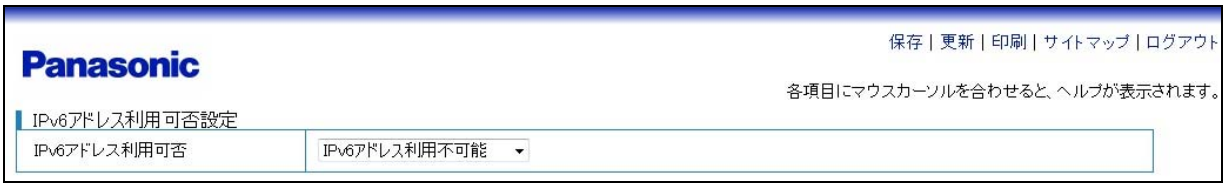


図4.7-47　IPv6 アドレス利用可否設定

［Passpoint 編集］画面（図 4.7-35）の［NAI Realm 設定］をクリックします。

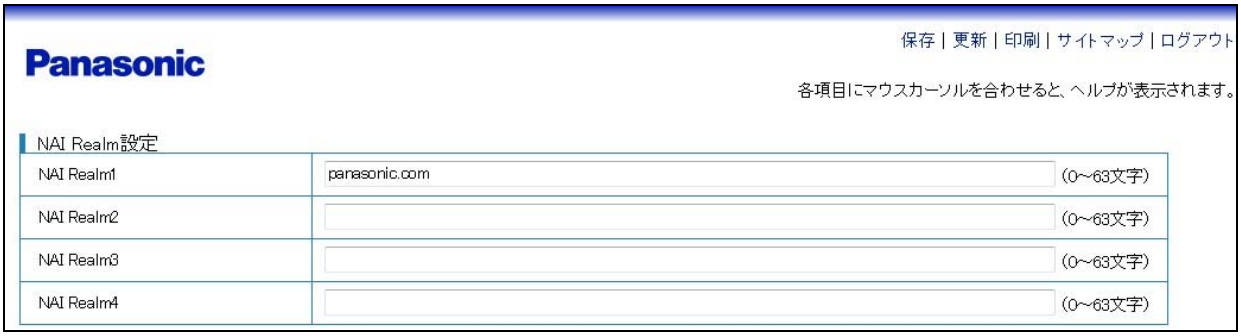


図4.7-48　NAI Realm 設定

［Passpoint 編集］画面（図 4.7-35）の［EAP メソッド設定］をクリックします。

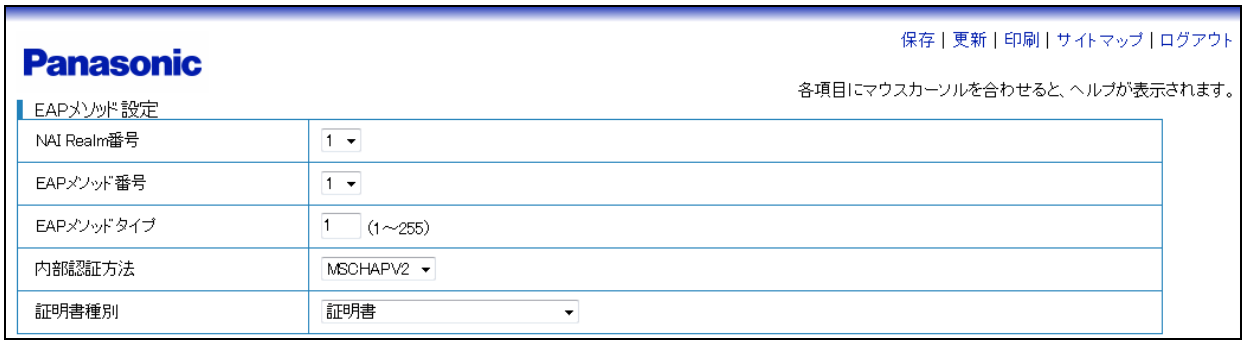


図4.7-49　EAP メソッド設定

［Passpoint 編集］画面（図 4.7-35）の［MCC 設定］をクリックします。

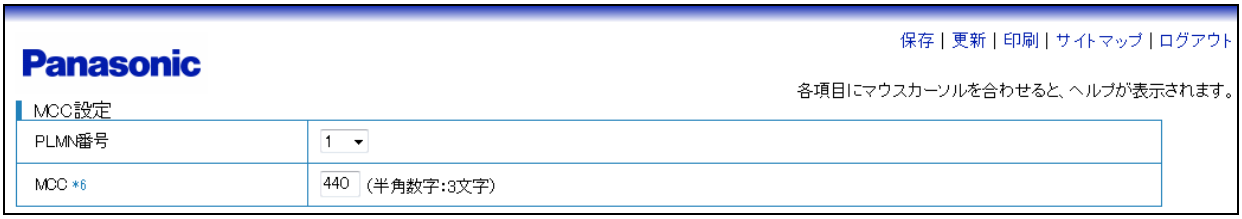


図4.7-50　MCC 設定

［Passpoint 編集］画面（図 4.7-35）の［MNC 設定］をクリックします。

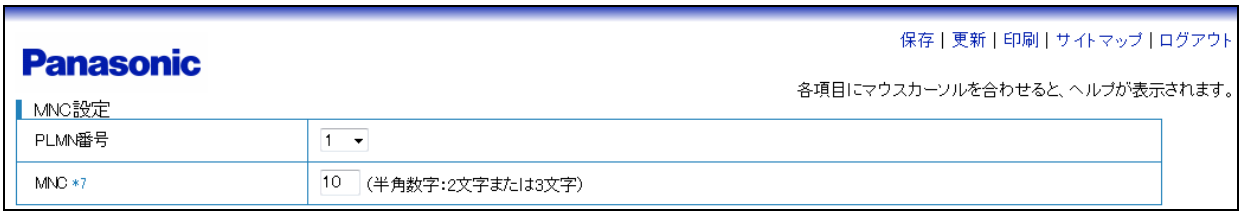


図4.7-51　MNC 設定

［Passpoint 編集］画面（図 4.7-35）の［ドメイン名設定］をクリックします。

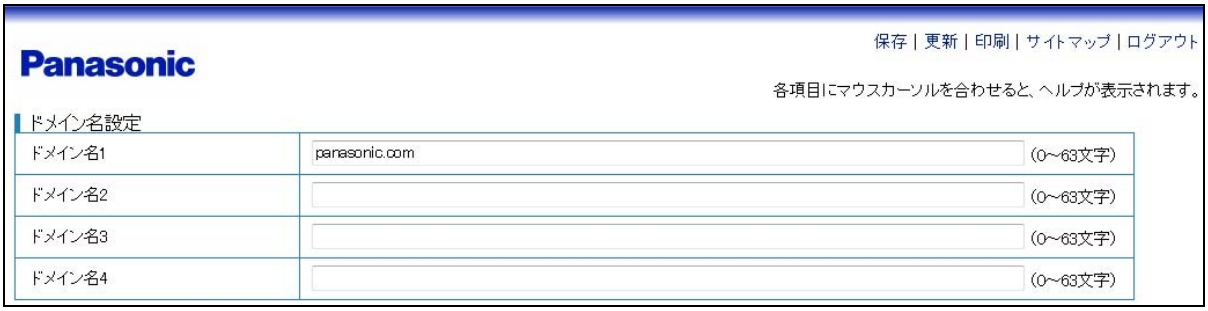


図4.7-52　ドメイン名設定

◆ Hotspot 2.0 ANQP エレメントに関する設定画面

［Passpoint 編集］画面（図 4.7-35）の［オペレータフレンドリー名設定］をクリックします。

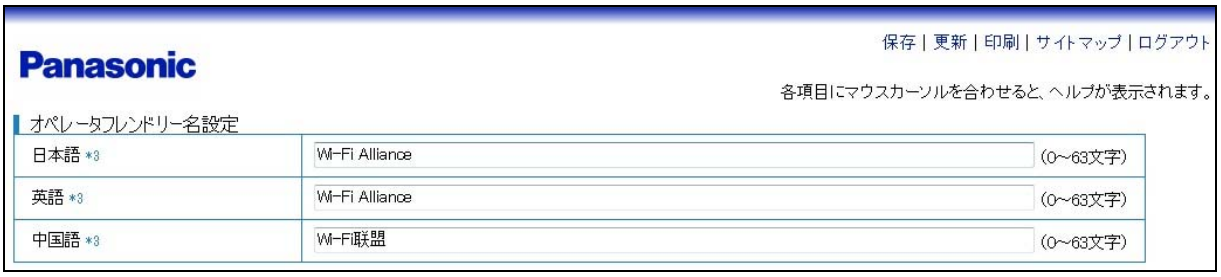


図4.7-53　オペレータフレンドリー名設定

［Passpoint 編集］画面（図 4.7-35）の［リンク速度設定］をクリックします。

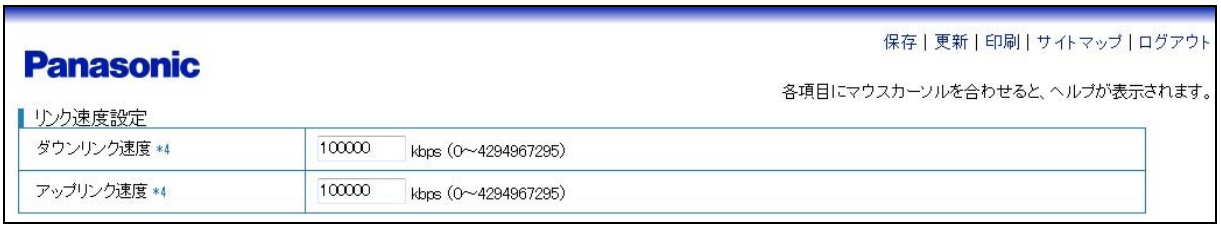


図4.7-54　リンク速度設定

［Passpoint 編集］画面（図 4.7-35）の［コネクション状態設定］をクリックします。

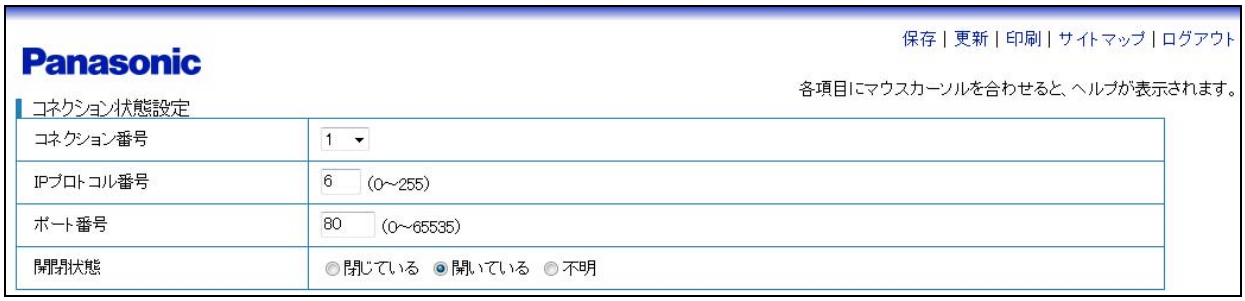


図4.7-55　コネクション状態設定

また、コンセントレータから端末へのグループアドレス宛てフレームの転送（Downstream Group-Address Forwarding）有無を切り替えることが可能です。

設定手順

手順1　〔SSID 管理〕　→　〔Passpoint 設定〕を選択します。

図4.7-56　メニュー（Passpoint 設定）

手順2　対象となる SSID の〔編集〕をクリックします。

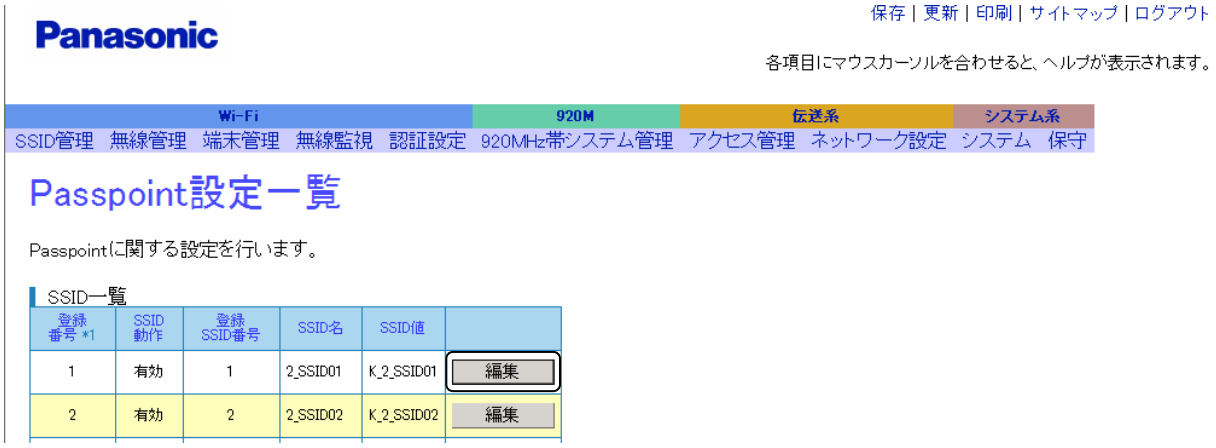


図4.7-57　Passpoint 設定一覧（SSID 一覧）

手順3　〔DGAF 設定〕をクリックします。

図4.7-58　Passpoint 編集

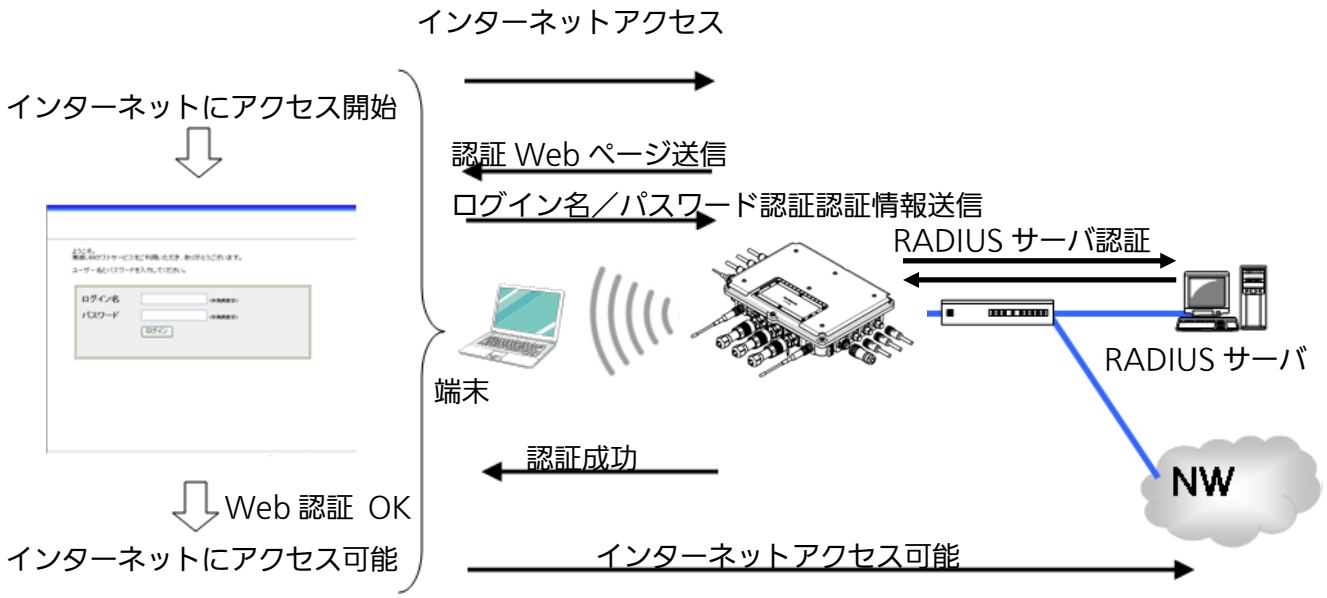
手順4　DGAF 設定を〔有効〕または〔無効〕にします。

DGAF 設定の初期値は〔有効〕です。DGAF 設定を〔無効〕にすると、〔SSID 編集〕画面の〔代理 ARP 応答動作〕の設定に関わらず、代理 ARP 応答動作が〔未学習端末宛てフレーム破棄〕となります。

図4.7-59　DGAF 設定

4.8　Web 認証

Web 認証では、ユーザが特別なソフトウェアを導入することなく、一般的に使用されている Web ブラウザのみを使用することで認証処理を行うことができます。ネットワーク利用の際には、Web ブラウザ上でログイン名とパスワードでの認証を行い、成功したユーザのみがネットワークにアクセスできるようになります。端末のブラウザに表示される認証画面の例を紹介します。



ここでは、Web 認証の各種設定方法を紹介します。

4.8.1　Web 認証一覧

設定手順

◆ Proxy 設定（Web 認証）

外部のネットワークにアクセスする際に、Web Proxy サーバを使用する環境においても、Web 認証が実施できるよう、Web Proxy サーバを登録します。SSID ごとに 16 個まで設定できます。

手順1　〔Wi-Fi〕 → 〔認証設定〕 → 〔Web 認証〕 → 〔Web 認証設定一覧〕を選択します。

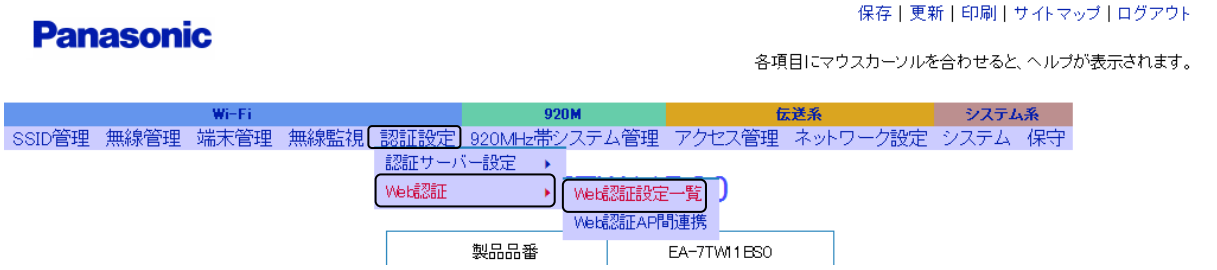


図4.8-1　メニュー（Web 認証設定一覧）

手順2　対象となる SSID の“Proxy 設定”を選択し、〔編集〕をクリックします。

※例として、登録番号 1 番に対して設定を行います。

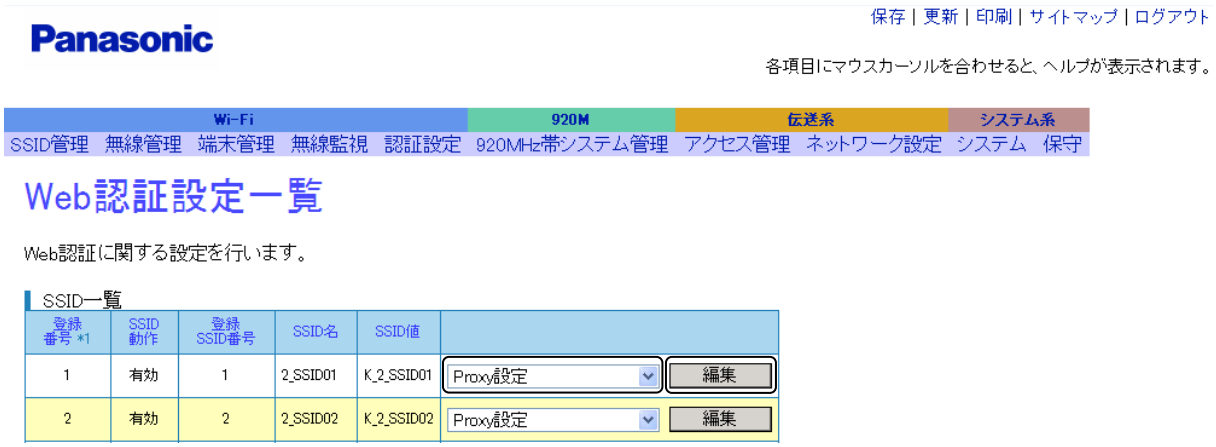


図4.8-2　Web 認証設定一覧

手順3　〔Proxy サーバ設定〕をクリックします。

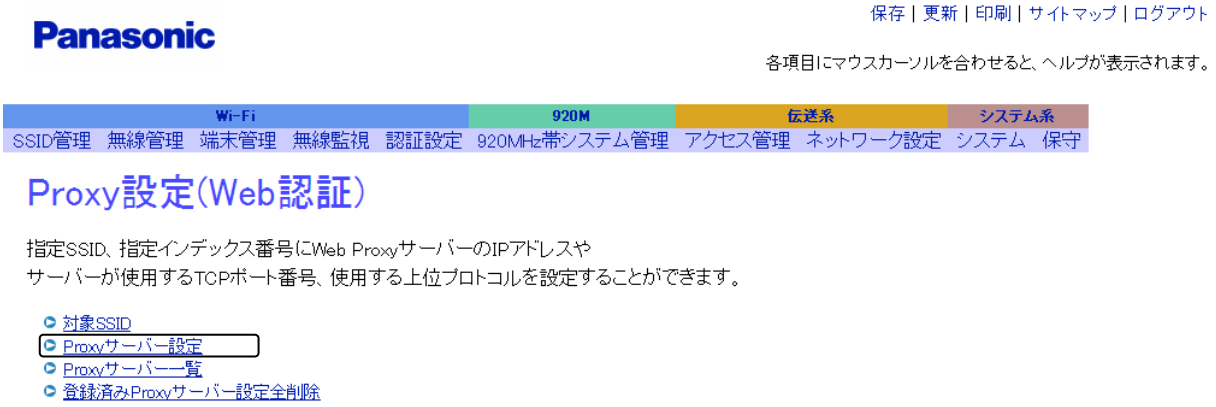


図4.8-3　Proxy 設定（Web 認証）

手順4　対象となる Proxy サーバの設定を行います。

例として、下記内容での設定を示します。

- 登録番号〔1〕を選択
- IP アドレスに　「1.72.197.139」を入力
- TCP ポート番号に「8080」を入力

画面最下部の〔設定〕をクリックし、設定を反映させます。

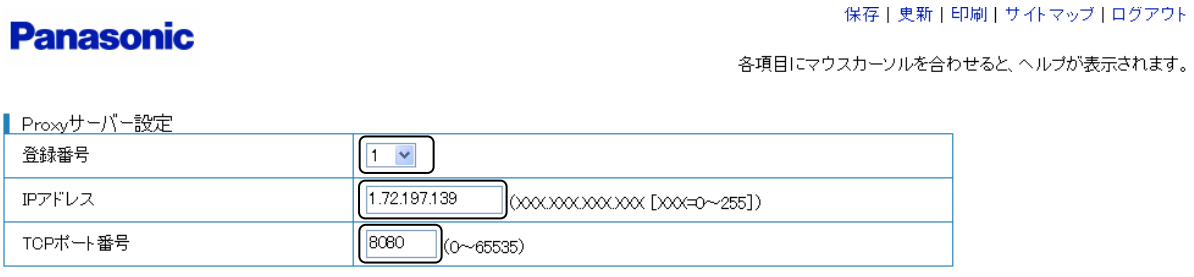


図4.8-4　Proxy サーバ設定

手順5　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

設定反映が正常に行われると、下記画面のように表示されます。

図4.8-5　Proxy サーバー一覧

設定手順

◆ 認証除外設定

指定した IP アドレスとの IP パケットの送受信に対しては、Web 認証状態が未認証であっても、端末と該当ホスト間の IP パケットを透過させることが可能です。認証除外設定対象のホストは、個々の SSID ごとに対し、最大 32 アドレスまで指定が可能です。対象ホストの情報は IP アドレスとサブネットマスク値の組み合わせで保持され、ネットワーク部が一致するホストとの送受信を透過させます。

手順1　〔Wi-Fi〕 → 〔認証設定〕 → 〔Web 認証〕 → 〔Web 認証設定一覧〕を選択します。

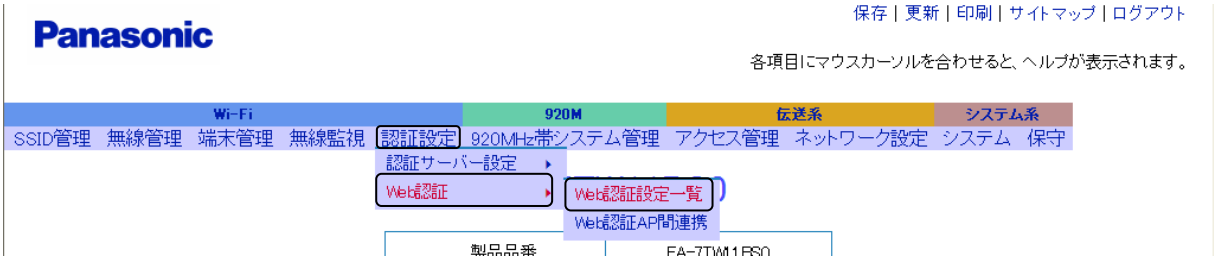


図4.8-6　メニュー（Web 認証設定一覧）

手順2　対象となる SSID の“認証除外設定”を選択し、〔編集〕をクリックします。

※ 例として、登録番号 2 番に対して設定を行います。

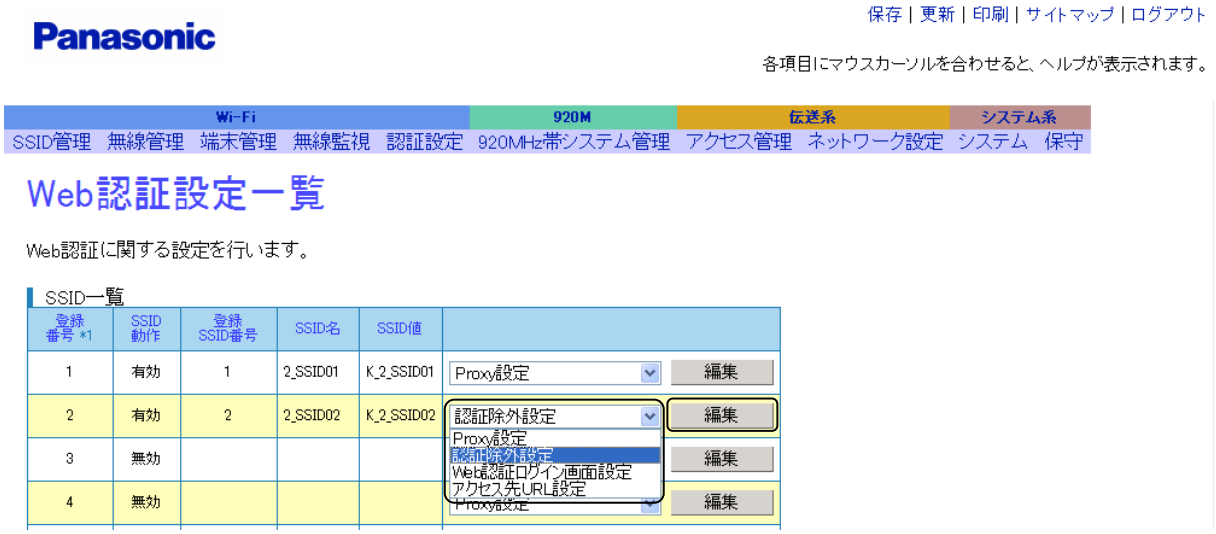


図4.8-7　Web 認証設定一覧表（認証除外設定）

手順3　〔認証除外アドレス設定〕をクリックします。

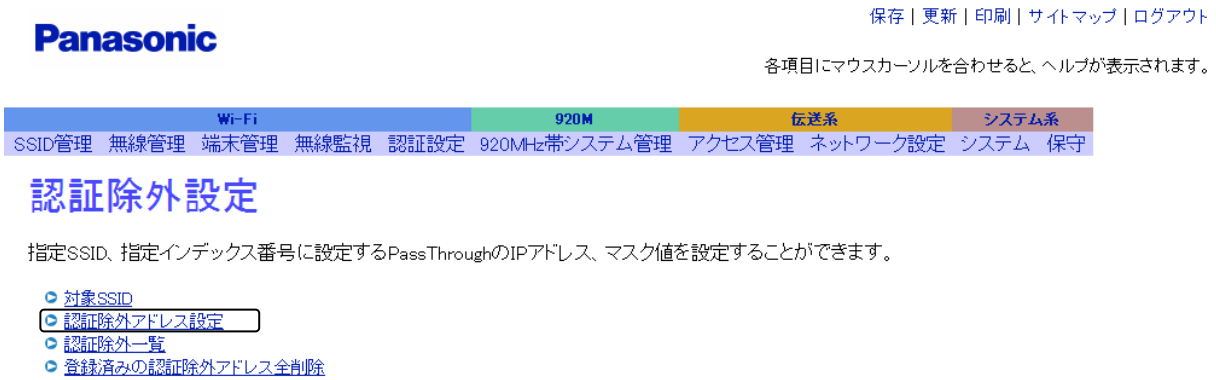


図4.8-8　認証除外設定（認証除外アドレス設定）

手順4　対象となる認証除外アドレスの設定を行います。

例として、下記内容での設定を示します。

- 登録番号〔2〕を選択
- IP アドレスに　「1.72.197.139」を入力
- マスク値に「255.255.255.0」を入力
  （フルアドレスマスクにより　ホストの指定も可能（マスクは中抜き可能））

画面最下部の〔設定〕をクリックし、設定を反映させます。

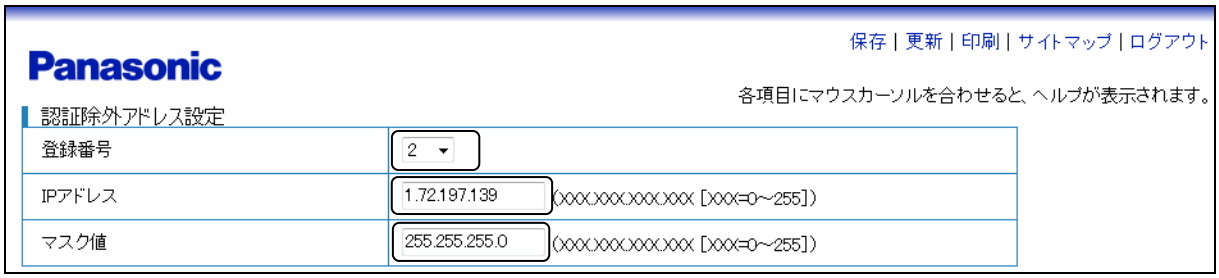


図4.8-9　認証除外アドレス設定

手順5　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

設定反映が正常に行われると、下記画面のように表示されます。

図4.8-10　認証除外一覧

設定手順

◆ Web 認証ログイン画面設定

通信事業者様ごとに個別のログインページのデザイン（ロゴなど）にできるよう、SSID ごとにログインページを設定することができます。

手順1　〔Wi-Fi〕 →〔認証設定〕 → 〔Web 認証〕 → 〔Web 認証設定一覧〕を選択します。対象となる SSID の“Web 認証ログイン画面設定”を選択し、〔編集〕をクリックします。

例として、登録番号 3 番に対して設定を行います。

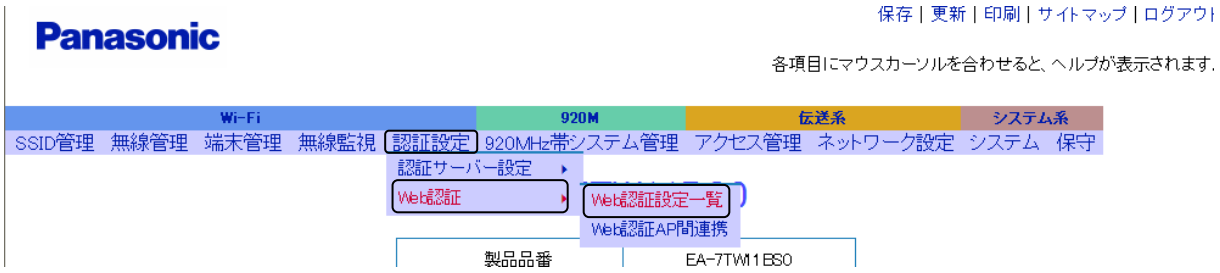


図4.8-11　メニュー（Web 認証設定一覧）

手順2　対象となる SSID の“Web 認証ログイン画面設定”を選択し、〔編集〕をクリックします。

例として、登録番号 3 番に対して設定を行います。

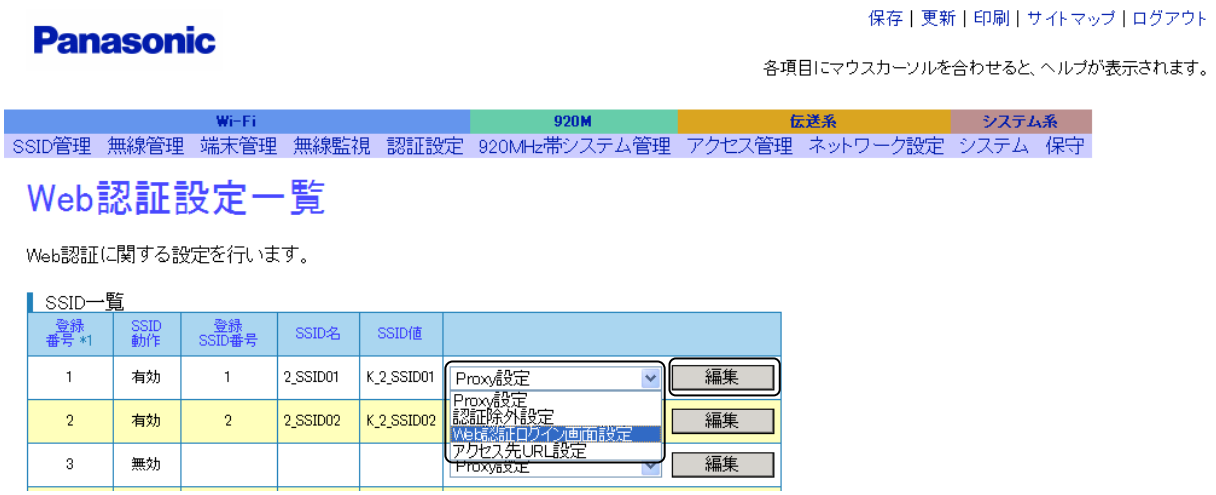


図4.8-12　Web 認証設定一覧表（Web 認証ログイン画面設定）

手順3　〔Web 認証ログイン画面設定〕をクリックします。

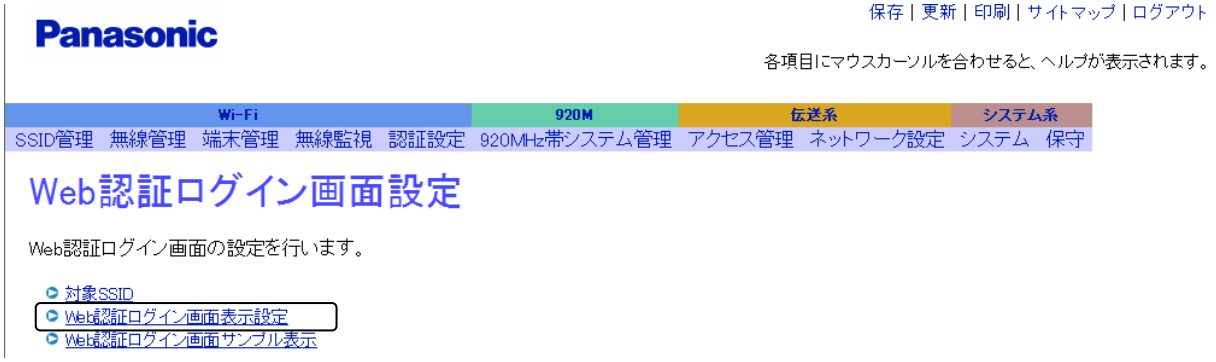


図4.8-13　Web 認証ログイン画面設定

手順4　対象となる Web 認証ログイン画面の設定を行います。

例として、下記内容での設定を示します。

- タイトルテキスト設定「Capital Portal Login」を入力
- 組織名設定に　「Panasonic Corporation」を入力
- ログインメッセージ設定に「ようこそ。
無線 LAN ゲストサービスをご利用いただき、ありがとうございます。

ユーザ名とパスワードを入力してください。」を入力
- フッタテキスト設定「ご利用方法は無線 LAN アクセス管理サイトへ」を入力
- メインロゴ URI 設定に　「http://127.0.0.1/main_logo.png」を入力
  ※メインロゴを使用しない場合は、メインロゴ URI 設定の入力欄を空欄にしてください。メインロゴを使用する場合、メインロゴ URI のホスト部に記載された IP アドレスは、認証除外設定が必要です。

- 利用条件メッセージ表示設定の〔有効〕を選択
- 利用条件メッセージ設定に　「本サービスのご利用にあたっては弊社が定める規約に
準拠していただく必要があります。

よろしければ、承認をチェックしてください。」を入力

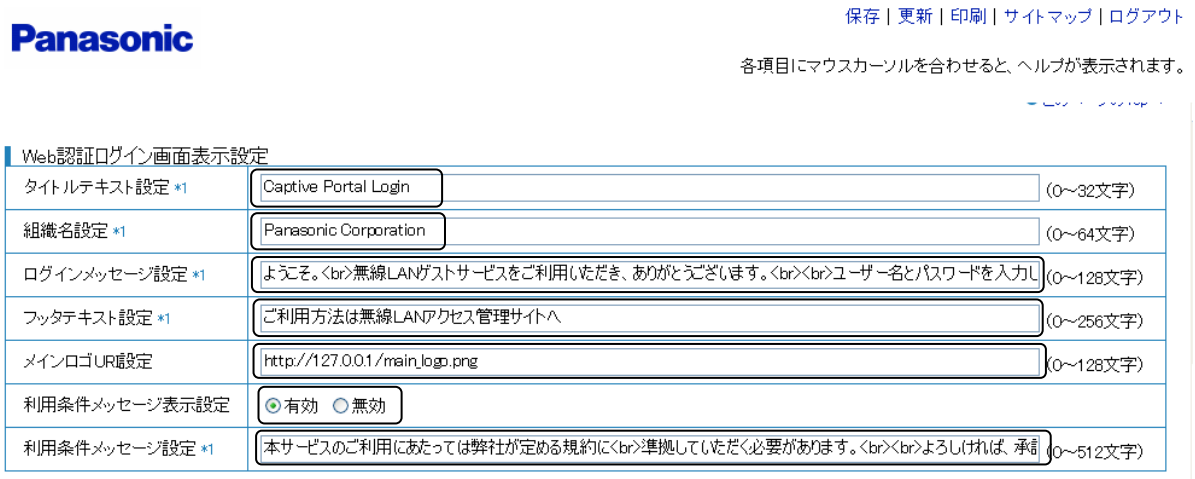


図4.8-14　Web 認証ログイン画面表示設定

手順5　上記設定終了後、画面最下部の〔設定〕をクリックし、設定を反映させます。

設定反映が正常に行われると、下部画面のように表示されます。

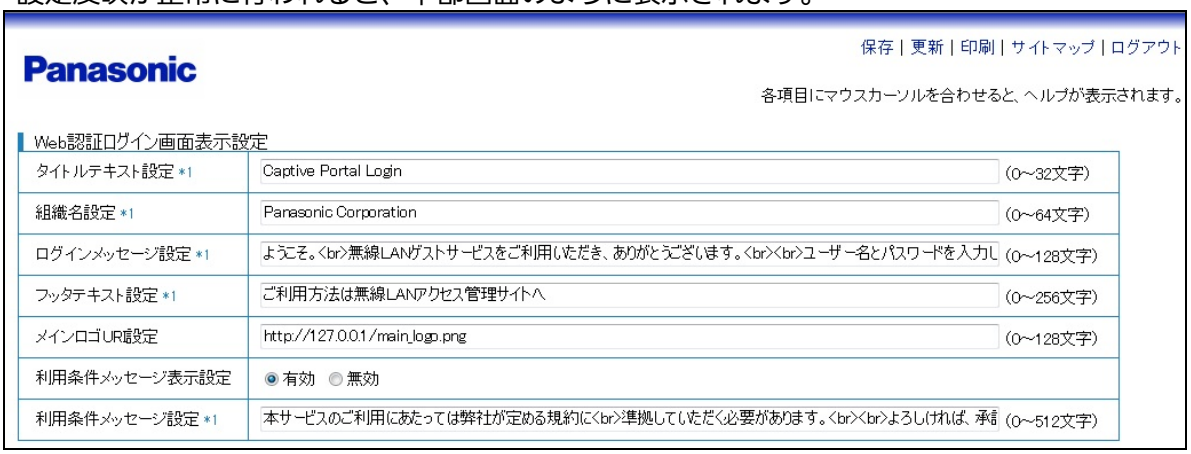


図4.8-15　Web 認証ログイン画面表示

手順6　〔Web 認証ログイン画面サンプル表示〕をクリックします。

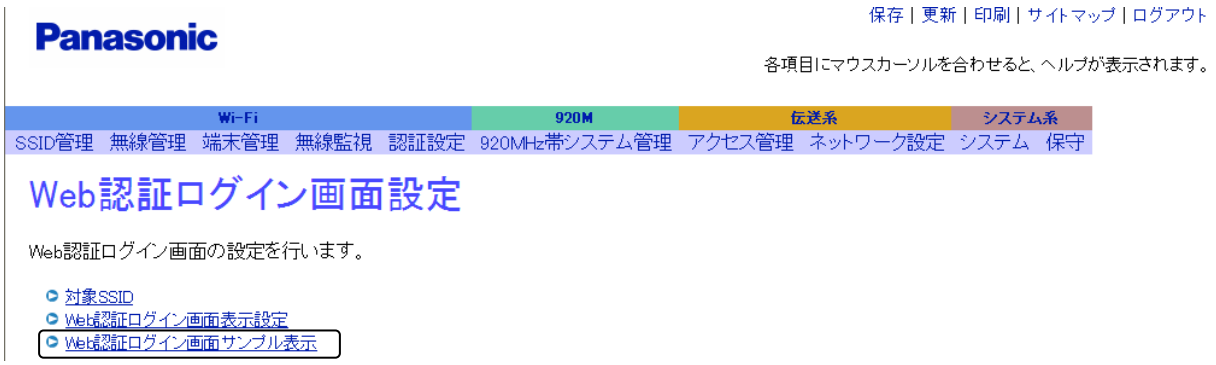


図4.8-16　Web 認証ログイン画面サンプル表示

手順7　サンプル画面表示の〔表示〕をクリックします。

図4.8-17　サンプル画面表示

手順8　手順 4 で設定したサンプル画面を確認することができます。

図4.8-18　サンプル画面

設定手順

◆ リダイレクト先 URL 設定

Web 認証成功時に端末にリダイレクトさせるアクセス先 URL を設定することができます。本設定は SSID ごとに 1 つずつ設定することが可能です。

手順1　〔認証設定〕 → 〔Web 認証〕 → 〔Web 認証設定一覧〕を選択します。

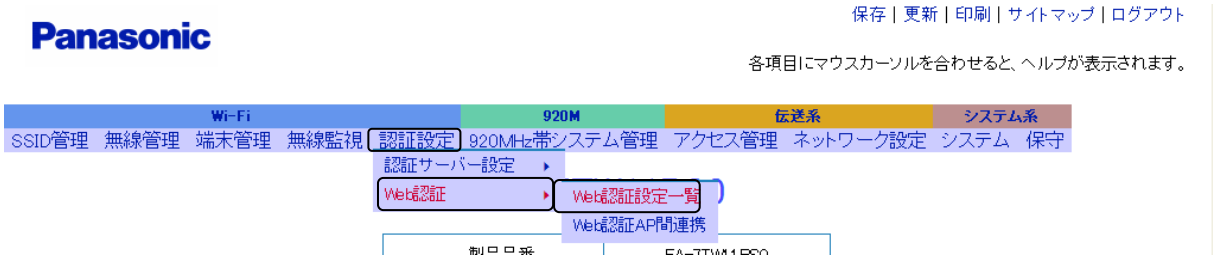


図4.8-19　メニュー（Web 認証設定一覧）

手順2　対象となる SSID の“アクセス先 URL 設定”を選択し、〔編集〕をクリックします。

例として、登録番号 2 番に対して設定を行います。

図4.8-20　Web 認証設定一覧表（アクセス先 URL 設定）

手順3　　認証セキュリティで使用するプロトコルの設定を行います。

例として、http プロトコルを使用する場合の設定を行います。

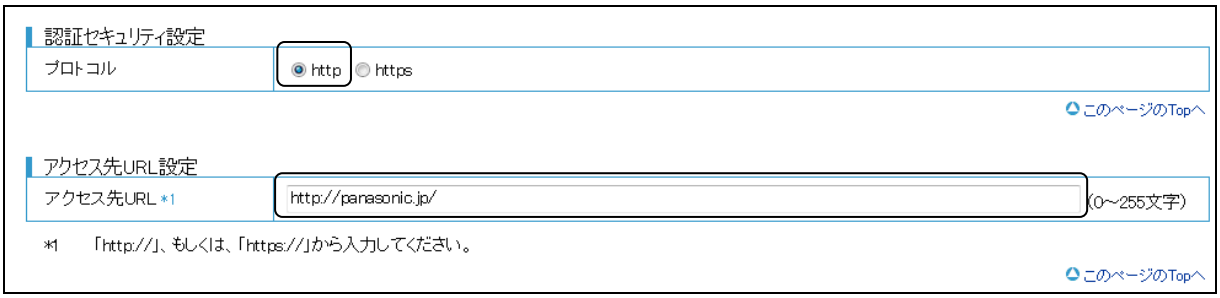


図4.8-21　　Web 認証詳細

手順4　　アクセス先 URL の設定を行います。

例として、[http://panasonic.jp/]をアクセス先 URL として設定を行います。
入力する URL は「http://」もしくは、「https://」から入力してください。
指定可能な最大 URL 長は 255 文字です。

手順5　　上記設定終了後、画面最下部の[設定]をクリックし、設定を反映させます。

設定反映が正常に行われると、下部画面のように表示されます。

図4.8-22　　Web 認証詳細設定画面

4.8.2　Web 認証 AP 間連携

端末が移動によりハンドオーバーして、接続先コンセントレータが変更した場合、接続先コンセントレータにおける Web 認証を省略することが可能です。そのため、初回接続先のコンセントレータにおいて、端末の Web 認証が完了した際に、周辺コンセントレータに対して当該端末が認証済みであることを通知することにより Web 認証情報を共有します。

コンセントレータは、端末接続時に Web 認証共有情報を参照し、接続端末の MAC アドレスが登録されている場合は、Web 認証済みとして扱い、改めて Web 認証処理を行うことなく、外部との通信を可能とさせます。

設定手順

端末が初回接続で Web 認証を行った際に、その Web 認証情報を通知するコンセントレータを設定します。通知先コンセントレータは 2 ヶ所まで設定できああます。

手順1　〔認証設定〕　→　〔Web 認証〕　→　〔Web 認証 AP 間連携〕を選択します。

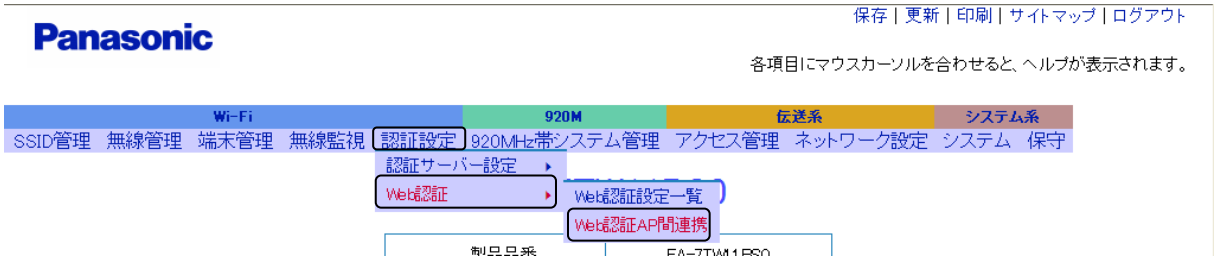


図4.8-23　メニュー（Web 認証 AP 間連携）

手順2　〔Web 認証生存時間〕をクリックします。

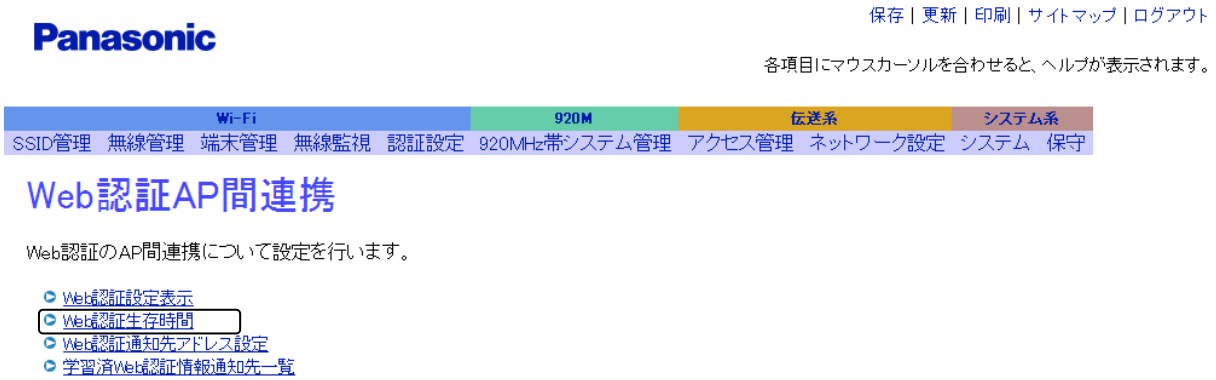


図4.8-24　Web 認証 AP 間連携

手順3　〔Web 認証生存時間〕の設定をします。

〔Web 認証生存時間〕を設定します。

例として、下記内容での設定を示します。

・ タイマー初期値に「1440」を入力

〔設定〕をクリックし、設定を反映させます。

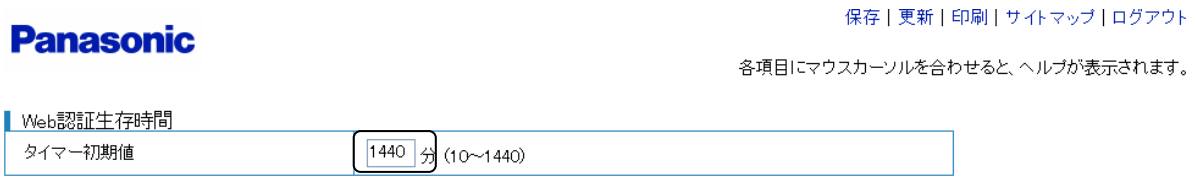


図4.8-25　Web 認証生存時間

手順4　〔Web 認証通知アドレス〕の設定をします。

〔Web 認証通知アドレス〕の設定を行います。

例として、下記内容での設定を示します。

・ 通知先番号〔1〕を選択

・ IP インターフェース番号〔2〕を選択

・ 通知先 IP アドレスに「192.168.0.200」を入力

〔設定〕をクリックし、設定を反映させます。

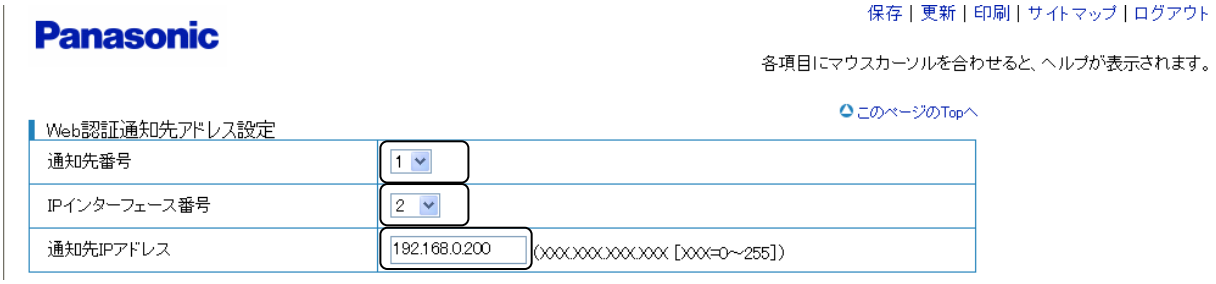
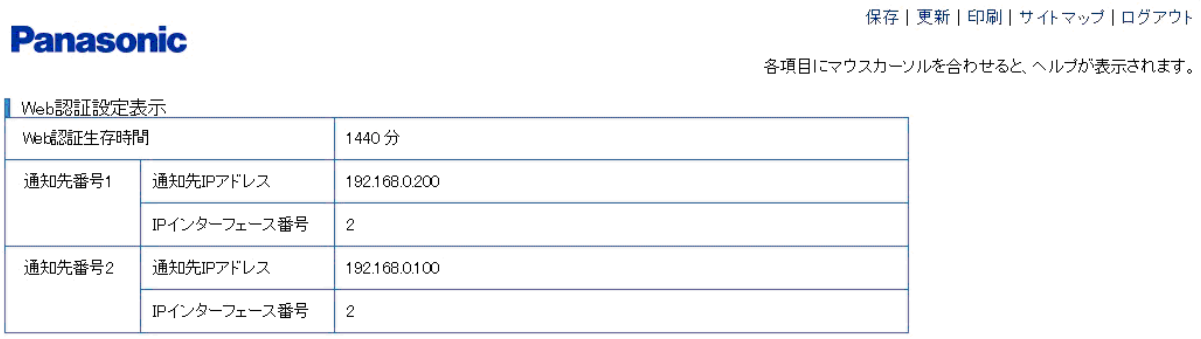


図4.8-26　Web 認証通知先アドレス設定

手順5　上記設定終了後、設定が反映させたことを確認します。

設定反映が正常に行われると、下記画面のように表示されます。



Web認証生存時間		1440 分
通知先番号1	通知先IPアドレス	192.168.0.200
	IPインターフェース番号	2
通知先番号2	通知先IPアドレス	192.168.0.100
	IPインターフェース番号	2

図4.8-27　Web 認証設定表示

4.9　PoE 給電

コンセントレータは、3 個の Ether ポートのうち 2 個(E2、E3)に接続された装置に対して PoE 給電ができます。

4.9.1　PoE 給電有効無効設定

コンセントレータは、PoE 給電できる Ethernet ポートを 2 ポート（E2/E3）有します。ただし、給電能力に限りがあるため、条件によっては接続された機器に給電することができません。さらに給電能力を超えた場合、コンセントレータにリセットが発生することがあります。

以下に給電能力の限界のパターンを示しますので、本内容を超えない範囲でシステム構成を行い、PoE 給電最大クラスの設定をしてください。

コンセントレータ電源種別	USB　未使用時	USB　使用時
DC48V(100W)	クラス 4 機器　2 台	クラス 4 機器　2 台
60W 対応 PoE インジェクタ（推奨品限定）	クラス 4 機器　1 台 または クラス 3 機器　2 台	クラス 3 機器　1 台 ＋ クラス 2 機器　1 台
PoE+（30W）	クラス 2 機器　1 台	給電不可
PoE（af） ※動作保証対象外	給電不可	給電不可

設定手順

手順1　〔システム〕　→　〔PoE 状態表示〕を選択します。

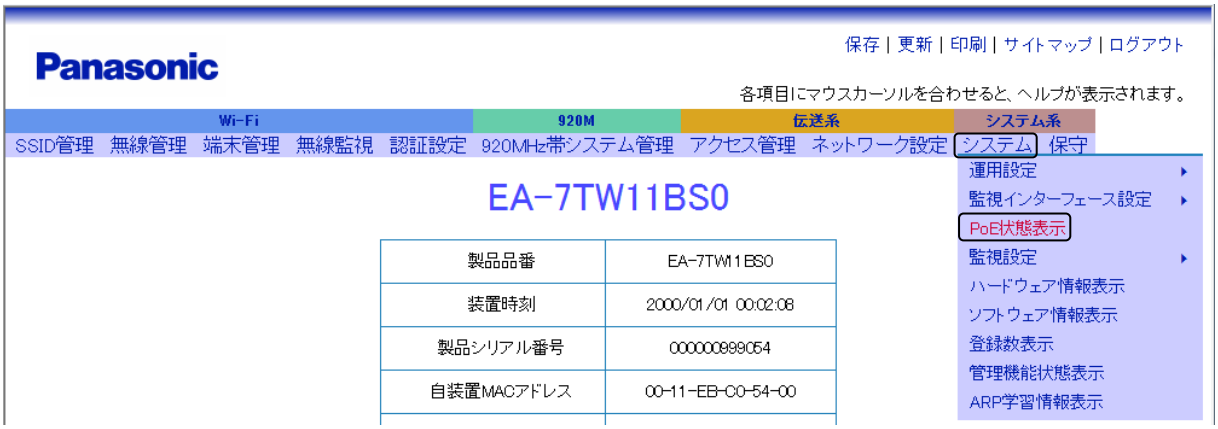


図4.10-1 メニュー（PoE 状態表示）

手順2　〔PoE 状態表示〕画面の〔PoE 給電設定〕を選択します。

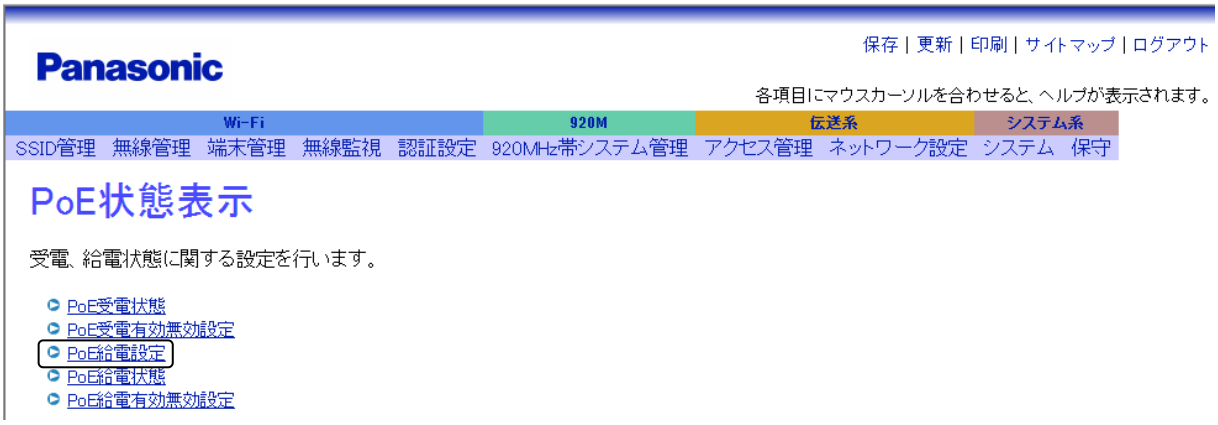


図4.10-2 PoE 給電設定

手順3　設定する”Ethernet ポート番号”を選択し、[表示]ボタンをクリックします。

例として、下記内容での設定を示します。

・ Ethernet ポート番号〔2〕を選択

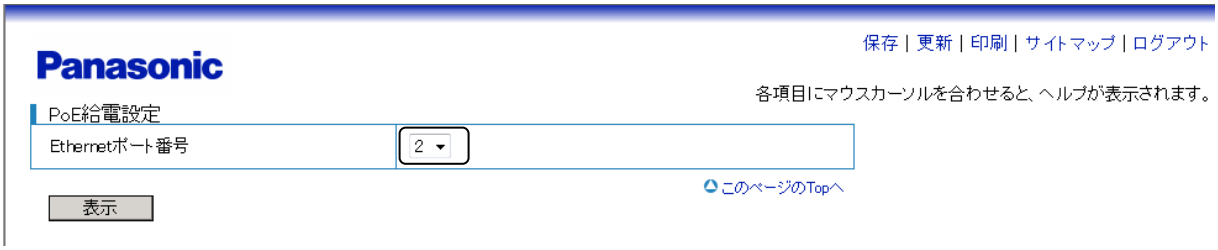


図4.10-3 PoE 給電設定

手順4　〔PoE 状態表示〕画面の〔PoE 給電有効無効設定〕を選択します。

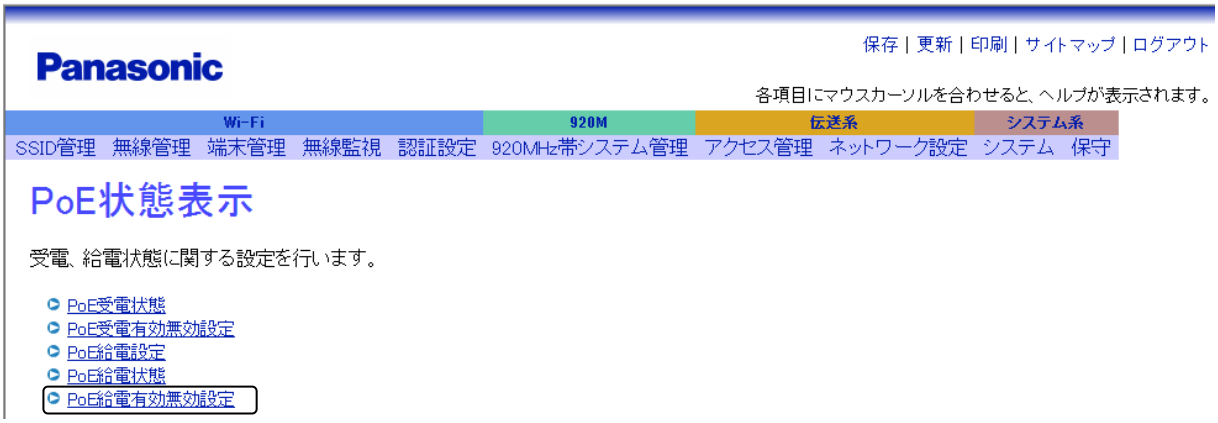


図4.10-4 PoE 給電有効無効設定

手順5　PoE 給電を有効にする場合は” PoE 給電有効無効設定”に[有効]を選択し、” PoE 給電最大クラス設定”に該当する Class（Class1～4）を選択します。PoE 給電を無効にする場合は” PoE 給電有効無効設定”に[無効]を選択します。選択後、[設定]ボタンをクリックします。

例として、下記内容での設定を示します。

- PoE 給電有効無効設定〔有効〕を選択
- PoE 給電最大クラス設定[Class3]を選択

なお、class0 のデバイスを接続する場合は、PoE 給電最大クラスは class3 を選択してください。

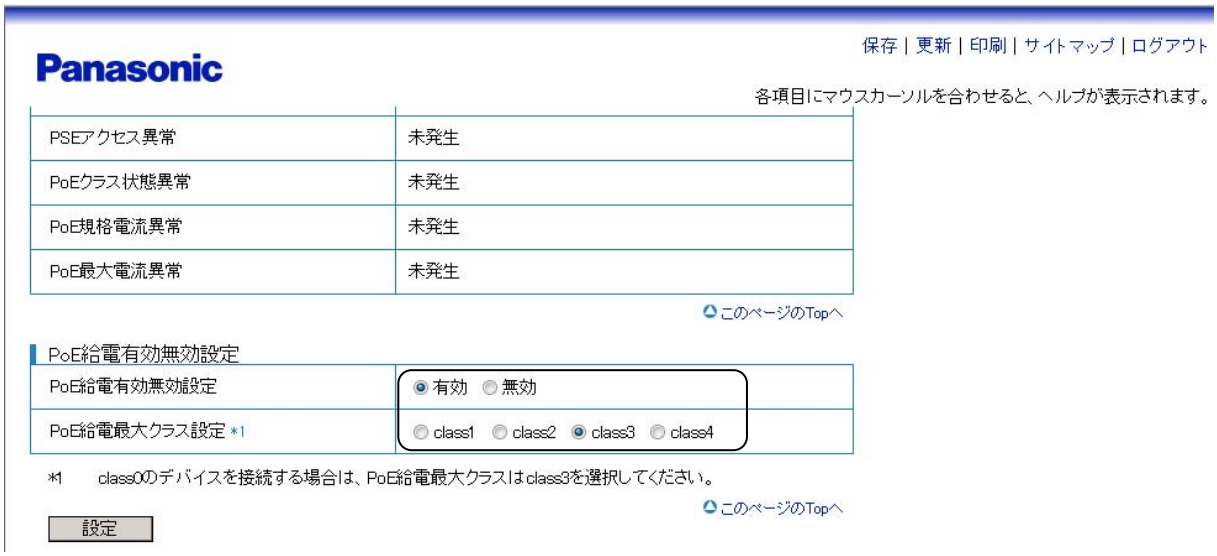


図4.10-5 PoE 給電有効無効設定

4.9.2　PoE 給電状態の確認

各 Ether ポート（LAN2、LAN3）に対し、PoE 給電状態の確認ができます。

設定手順

手順1　〔システム〕　→　〔PoE 状態表示〕を選択します。

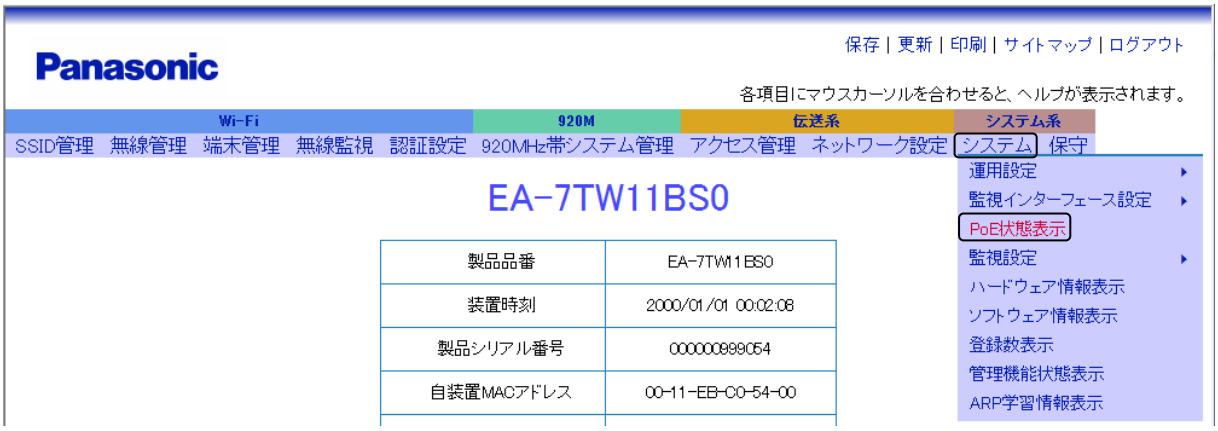


図4.10-6 メニュー（PoE 状態表示）

手順2　〔PoE 状態表示〕画面の〔PoE 給電設定〕を選択します。

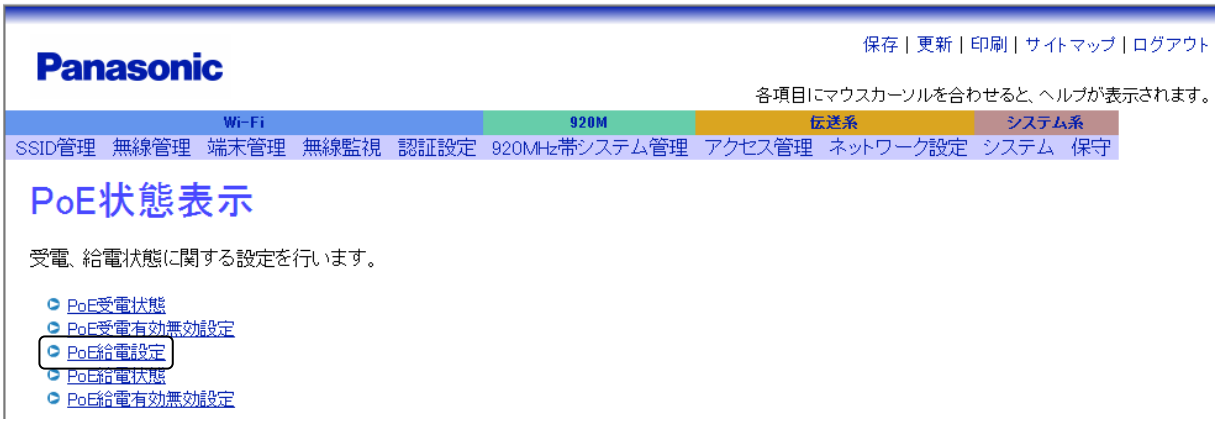


図4.10-7 PoE 給電設定

手順3　設定する”Ethernet ポート番号”を選択し、[表示]ボタンをクリックします。

例として、下記内容での設定を示します。

・ Ethernet ポート番号〔2〕を選択

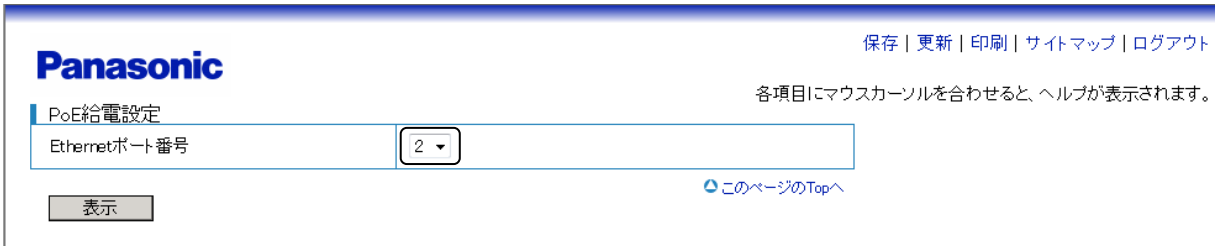


図4.10-8 PoE 給電設定

手順4　〔PoE 状態表示〕画面の〔PoE 給電状態〕を選択すると、PoE 給電状態が表示されます。

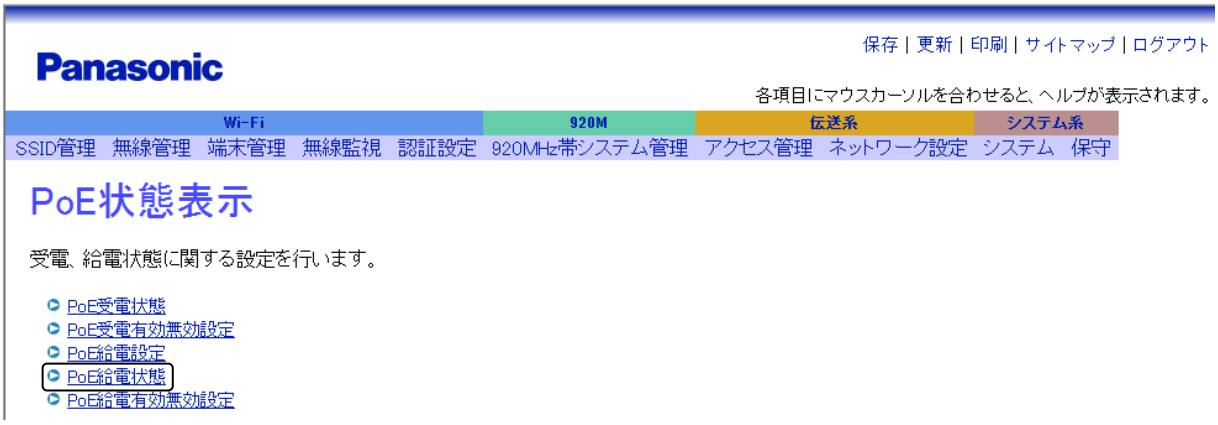


図4.10-9 PoE 給電状態

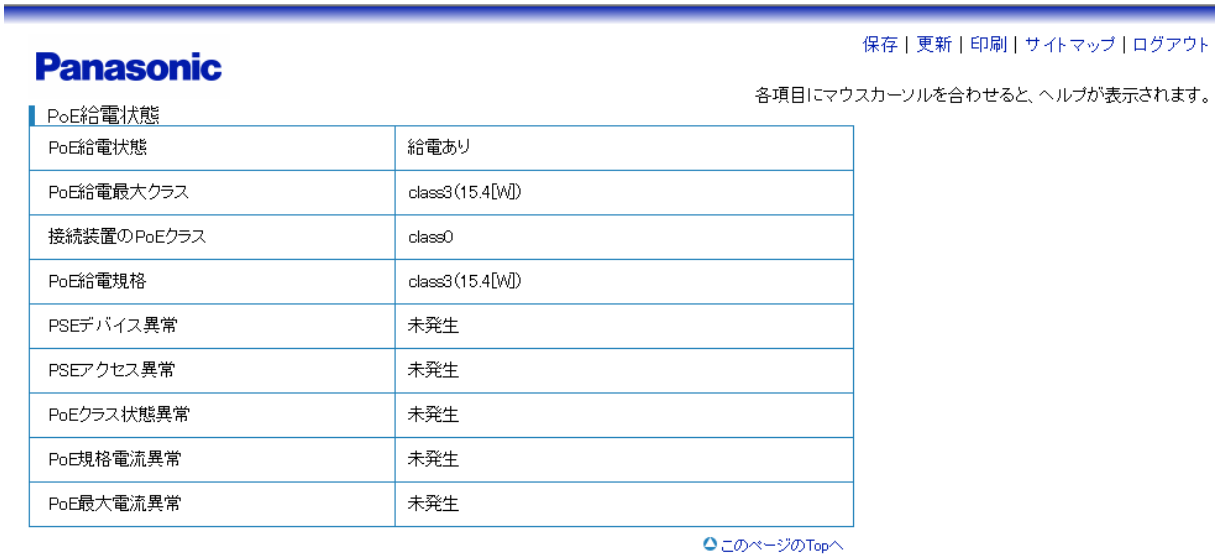


図4.10-10 PoE 給電状態

4.10　WAN 回線制御

WAN 回線制御機能として、「回線冗長化」および「リンクパススルー」について説明します。

■回線冗長化

設定手順

手順1　〔伝送系〕　→　〔ネットワーク設定〕　→　〔WAN 回線制御〕を選択します。

図4.10-1 メニュー（WAN 回線制御）

手順2　〔WAN 回線制御〕画面の〔WAN 回線設定〕を選択します。

図4.10-2 WAN 回線制御

手順3　主回線および副回線の設定を行い、[設定]ボタンをクリックします。

例として、下記内容での設定を示します。

- 主回線〔無線ブリッジ〕を選択
- 副回線〔Ethernet ポート 1〕を選択

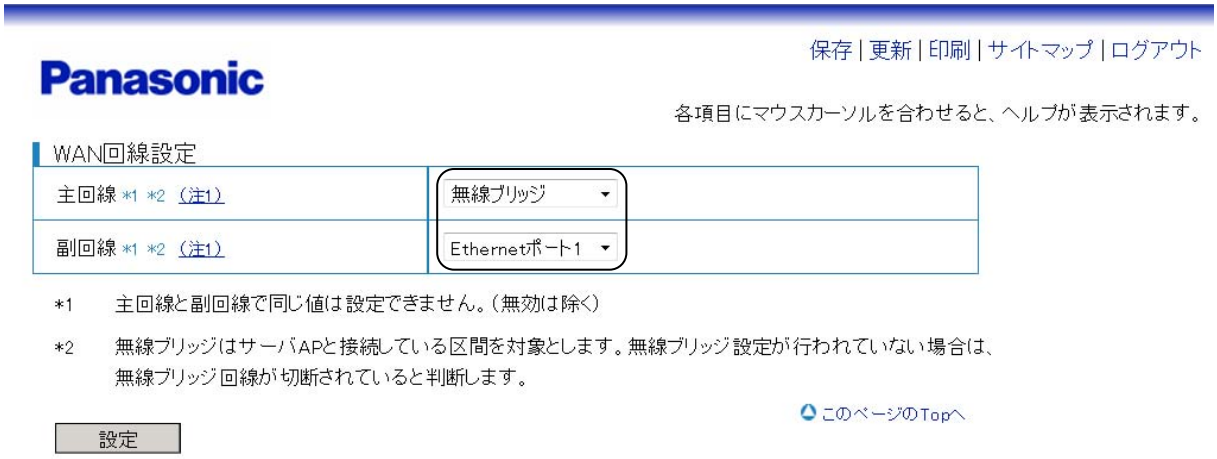


図4.10-3 WAN 回線設定

手順4　主回線の監視設定を行います。設定後、図 4-3.33 の下にある[設定]ボタンをクリックします。

例として、Layer2/Layer3 監視方式で、60 秒ごとに 3 回接続監視を行う場合の設定を示します。

- 接続監視方式〔Layer2/Layer3〕を選択
- IP インターフェース番号〔1〕を選択
- 接続監視対象 IP アドレス〔10.10.10.10〕を設定
- 接続監視間隔〔60〕秒を設定
- 接続監視パケット応答待ち時間〔5〕秒を設定
- 接続監視連続失敗上限〔3〕回を設定

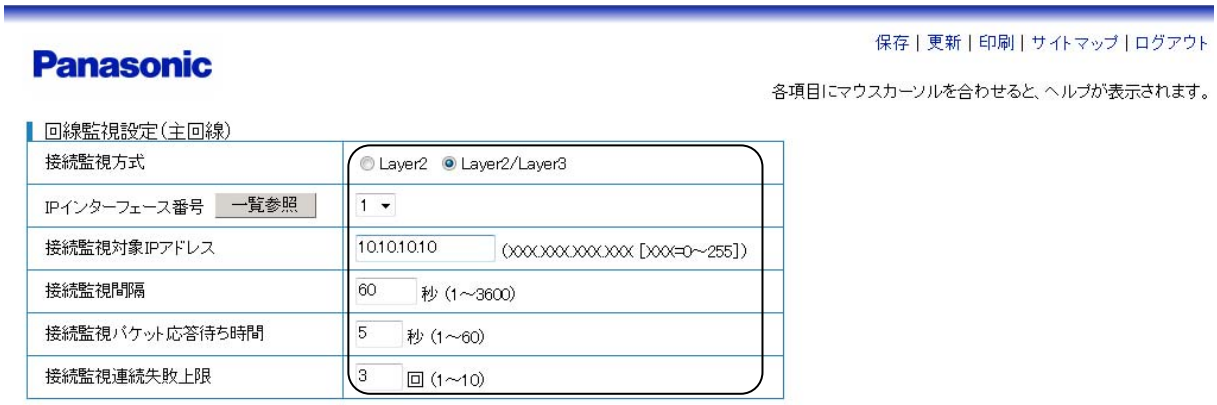


図4.10-4 主回線 回線監視設定

手順5　副回線の監視設定を行います。設定後、[設定]ボタンをクリックします。

例として、Layer2 監視方式で、60 秒ごとに 3 回接続監視を行う場合の設定を示します。

- 接続監視方式〔Layer2〕を選択
- 接続監視間隔〔60〕秒を設定
- 接続監視パケット応答待ち時間〔5〕秒を設定
- 接続監視連続失敗上限〔3〕回を設定

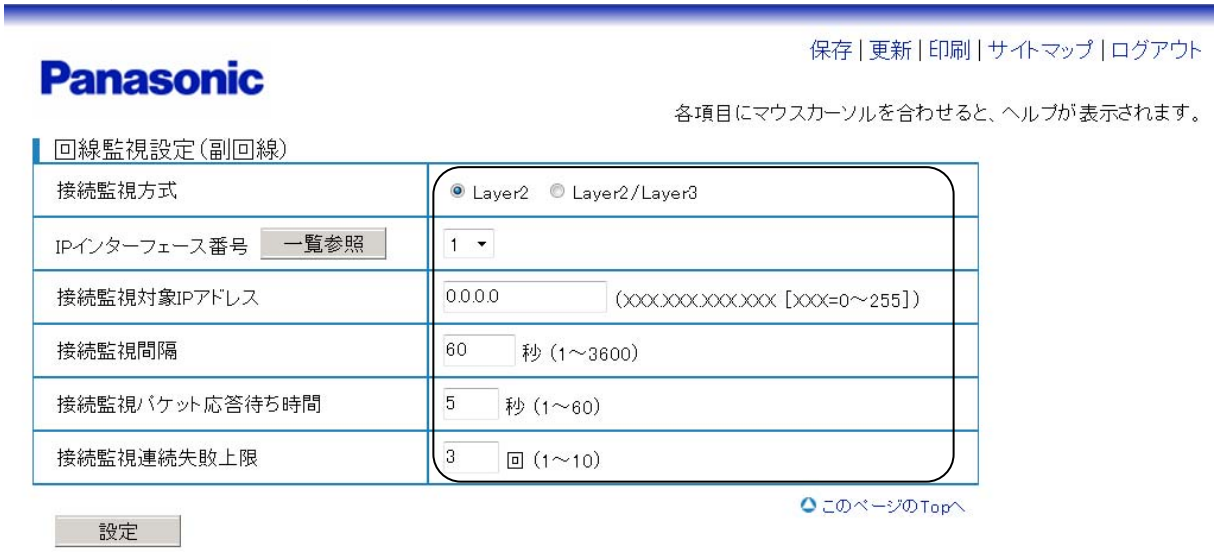


図4.10-5 副回線 回線監視設定

手順6　回線冗長化の設定を行います。[設定]ボタンをクリックします。

例として、回線切り替え時に監視を再開する遅延時間を 20 秒に、副回線で動作しているとき、主回線が復旧した場合の切り戻し時間を 60 分にする場合の設定を示します。

- 回線冗長化機能〔有効〕を選択
- 回線切り替え遅延時間〔20〕秒を設定
- 回線自動切り戻し機能〔有効〕を設定
- 回線自動切り戻しタイマー〔60〕分を設定

図4.10-6 回線冗長化設定

手順7　リンクパススルーの設定を行います。[設定]ボタンをクリックします。

例として、WAN 回線が切断して、3 秒後にリンクパススルーを実施する場合の設定を示します。

・ リンクパススルー機能〔有効〕を選択

・ 検出遅延時間〔3〕秒を設定

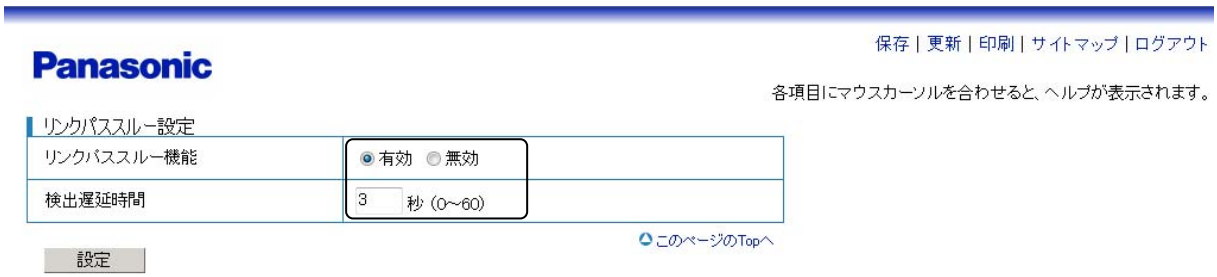


図4.10-7 リンクパススルー設定

4.11　端末間通信禁止

端末間通信禁止について説明します。

設定手順

手順1　〔伝送系〕　→　〔ネットワーク設定〕　→　〔VLAN 設定〕
→　〔端末間通信禁止設定〕を選択します。

図4.11-1 メニュー（端末間通信禁止設定）

手順2　〔端末間通信禁止設定〕画面の〔端末間通信禁止設定〕をクリックします。

端末間の通信を禁止するフレームを以下の条件で設定できます。

- 全フレーム
- タグなしフレーム
- VLAN-ID 単位

全フレームおよびタグなしフレームは〔端末間通信禁止設定〕で設定します。
VLAN-ID 単位は、〔VLAN-ID 追加〕で設定します。
ここでは、全フレーム設定を説明します。

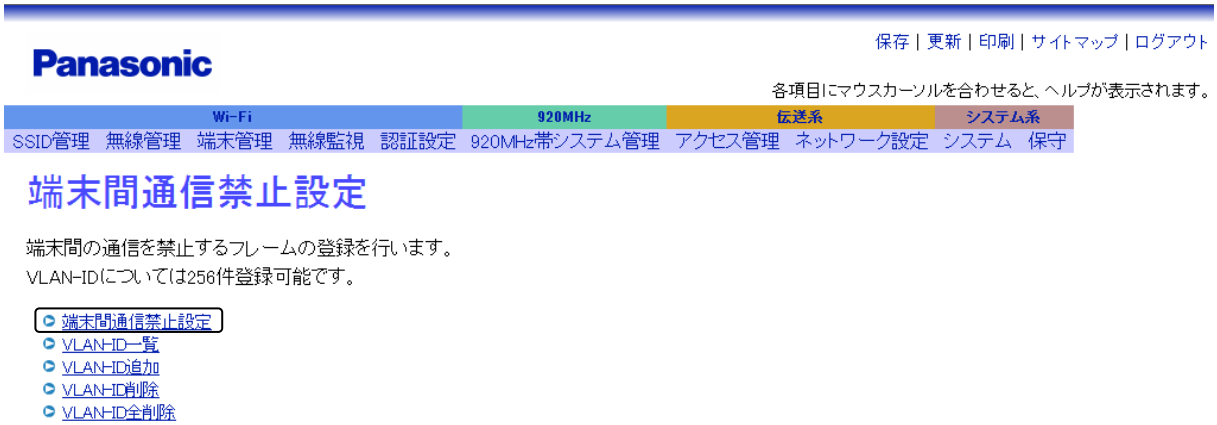


図4.11-2 端末間通信禁止設定画面

手順3　フレームごとの端末間通信禁止設定を選択し、[設定]ボタンをクリックします。

例として、下記内容での設定を示します。

- 全フレーム〔有効〕を選択
- タグなしフレーム〔無効〕を選択

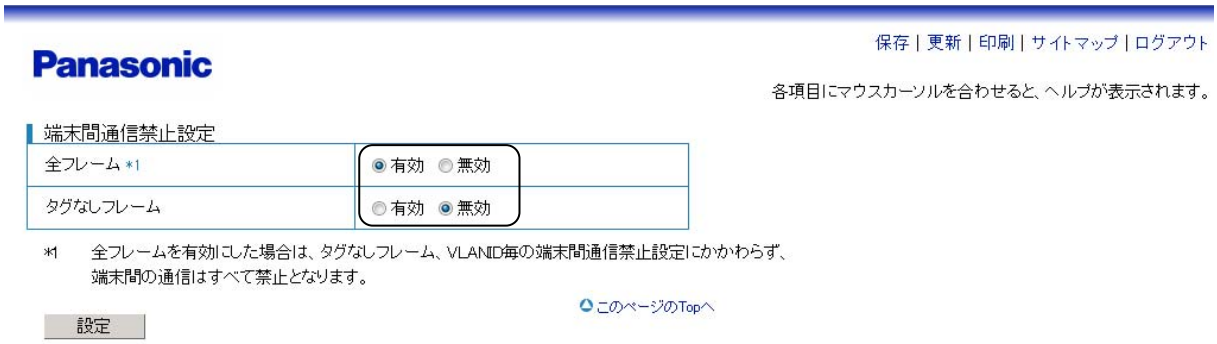


図4.11-3 端末間通信禁止設定

4.12　その他の機能

その他の機能として、SSID ごとに設定を行う「アグリゲーション」、「LDPC 符号化」ならびに「送信ビームフォーミング」について説明します。

設定手順

手順4　〔Wi-Fi〕　→　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

図4.12-1　メニュー（SSID 設定）

手順5　〔SSID 一覧〕をクリックします。

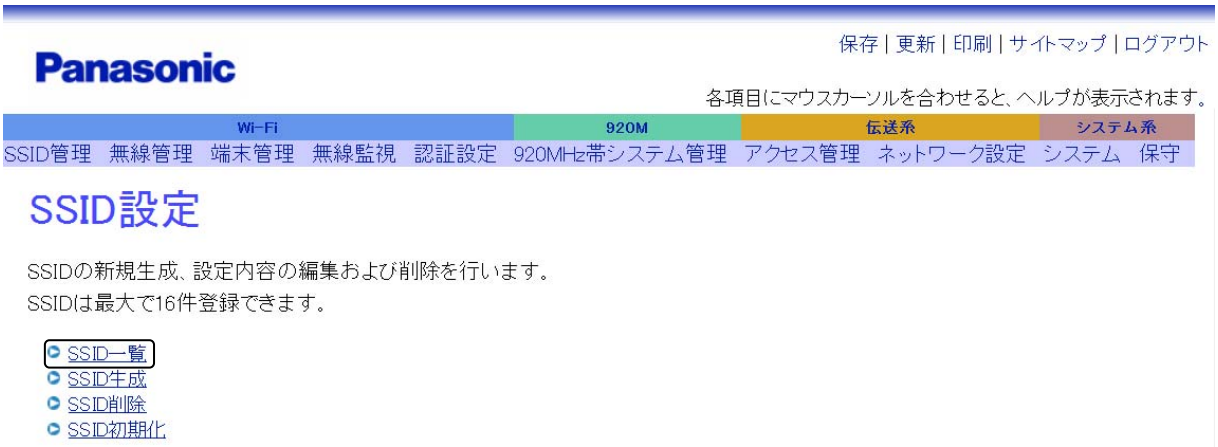


図4.12-2　SSID 設定

手順6　対象となる SSID の〔編集〕をクリックします。

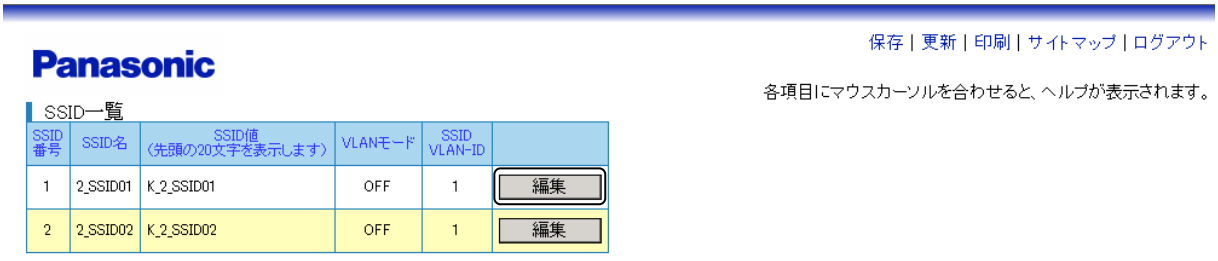


図4.12-3　SSID 一覧

〔SSID 編集〕画面（図 4.9-4）が表示されます。前述の機能設定はこちらより行います。

図4.12-4　SSID 編集

■アグリゲーション

高速化通信を実現するため、フレームを連結する方式として、A-MPDU と A-MSDU の 2 種類が存在しています。

アグリゲーションでは、「OFF」「A-MPDU」「A-MSDU」「A-MPDU＋A-MSDU」（4 パターン）のいずれかを選択します。

〔SSID 編集〕画面（図 4.9-4）の〔アグリゲーション〕をクリックします。

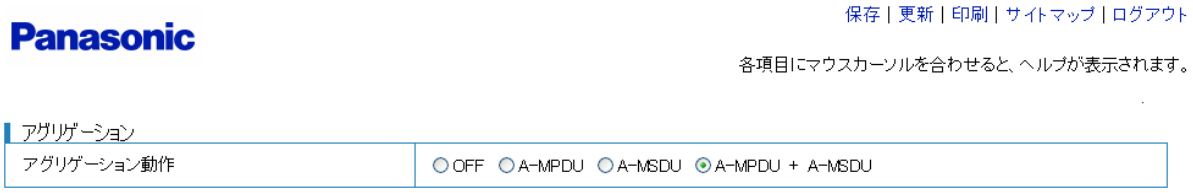


図4.12-5　アグリゲーション

■LDPC 符号化

アソシエーション時に、コンセントレータで〔LDPC 符号化〕が有効、かつ端末が LDPC 対応である場合に限り、LDPC 符号を使用します。〔無効〕を選択した場合は「畳み込み符号を使用」となります。

〔SSID 編集〕画面（図 4.9-4）の〔LDPC 符号化〕をクリックします。

図4.12-6　LDPC 符号化

■送信ビームフォーミング

コンセントレータで、送信ビームフォーミングの〔有効〕を選択した場合、単一フレームを複数のアンテナから送信する際、各アンテナから送信する信号の位相を制御することで、受信クライアントで信号のパワーが最大になるようにします。〔無効〕を選択した場合は送信ビームフォーミング機能は有効になりません。

〔SSID 編集〕画面（図 4.9-4）の〔送信ビームフォーミング〕をクリックします。

図4.12-7　送信ビームフォーミング

第５章　VPN ネットワーク対応

VPN ネットワーク構築の設定手順について、説明します。

5.1　L2TP over PPPoE ネットワーク接続での設定

ここでは、PPPoE でインターネットに接続している 2 つの拠点を L2TP で結ぶ VPN 構築例を紹介します。

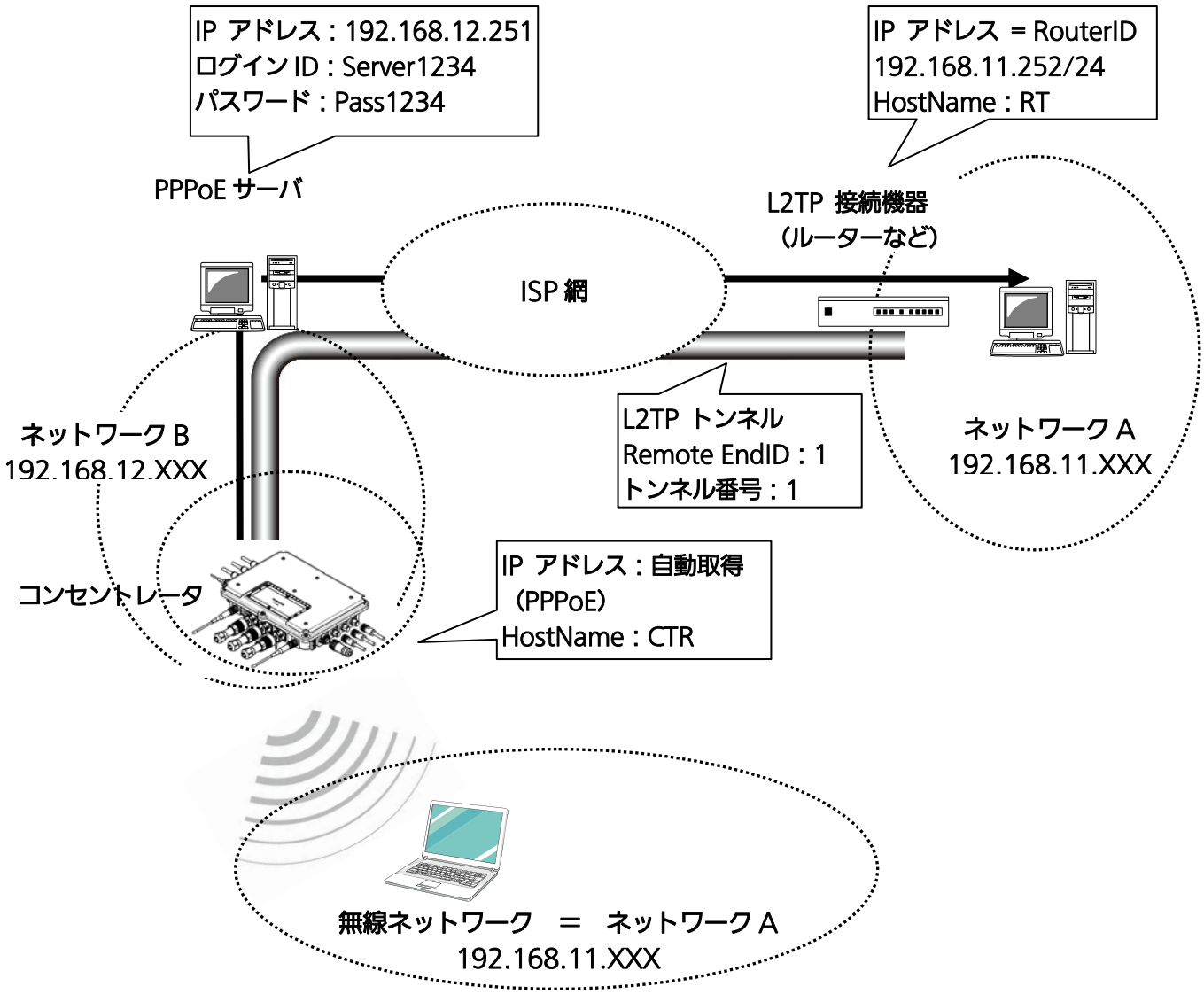


図5.1-1　　ネットワーク構成例（L2TP over PPPoE）

図 5.1-1（L2TP over PPPoE）を構築するための設定は、以下の手順で行います。

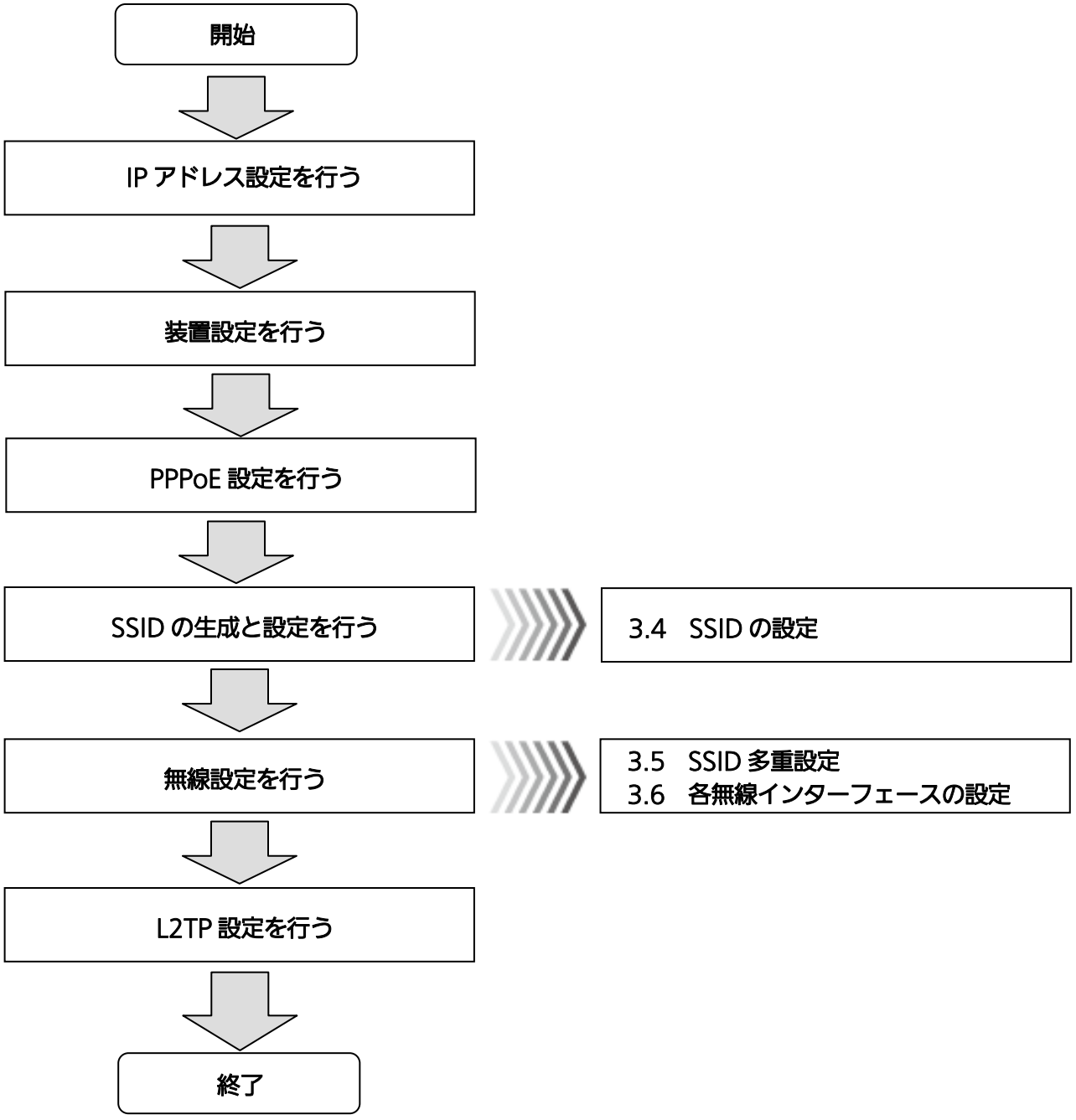


図5.1-2　ネットワーク構成手順（L2TP over PPPoE）

設定手順

◆IP アドレス設定

手順1　〔システム系〕　→　〔システム設定〕　→　〔監視インターフェース設定〕
→　〔IP アドレス設定〕を選択します。

図5.1-3　メニュー（IP アドレス設定）

手順2　対象となる IP インターフェース 1 番の〔編集〕をクリックします。

図5.1-4　IP アドレス設定

手順 3 ～ 手順 4 は〔IP アドレス編集〕画面（図 5.1-5）より各種設定を行います。

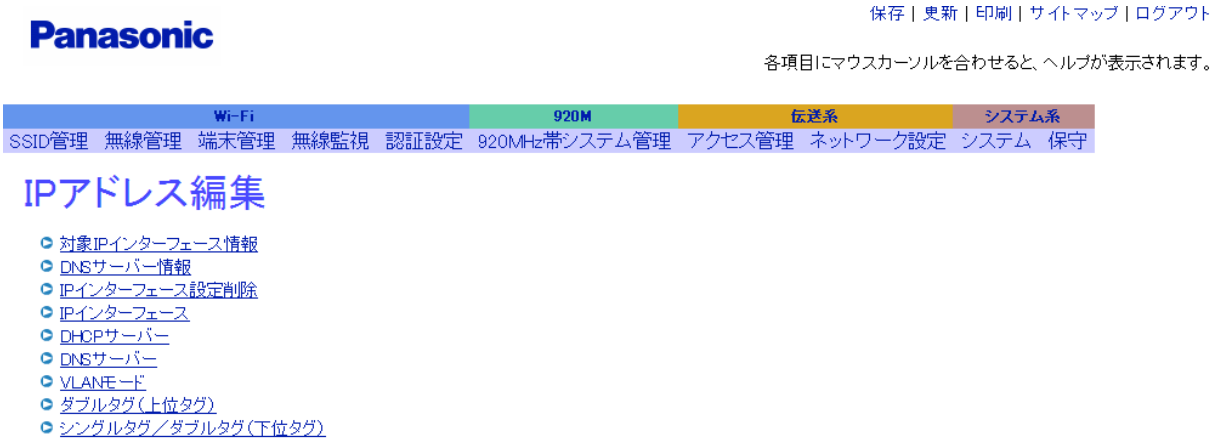


図5.1-5　IP アドレス編集

手順3　〔IP アドレス編集〕画面（図 5.1-5）の IP インターフェースをクリックし、IP インターフェース 1 番に対して下記設定を行います。

- インターフェースの〔有効〕を選択
- 動作モードの〔PPP〕を選択

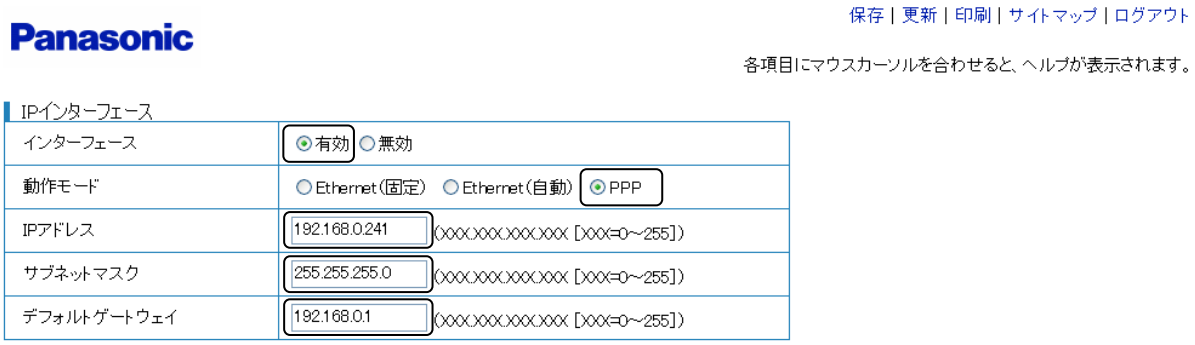


図5.1-6　IP インターフェース

手順4　画面最下部の〔設定〕をクリックし、設定を反映させます。

◆装置設定

手順5　〔伝送系〕　→　〔システム設定〕　→　〔運用設定〕　→　〔装置設定〕を選択します。

図5.1-7　メニュー（装置設定）

手順6　〔装置情報〕をクリックします。

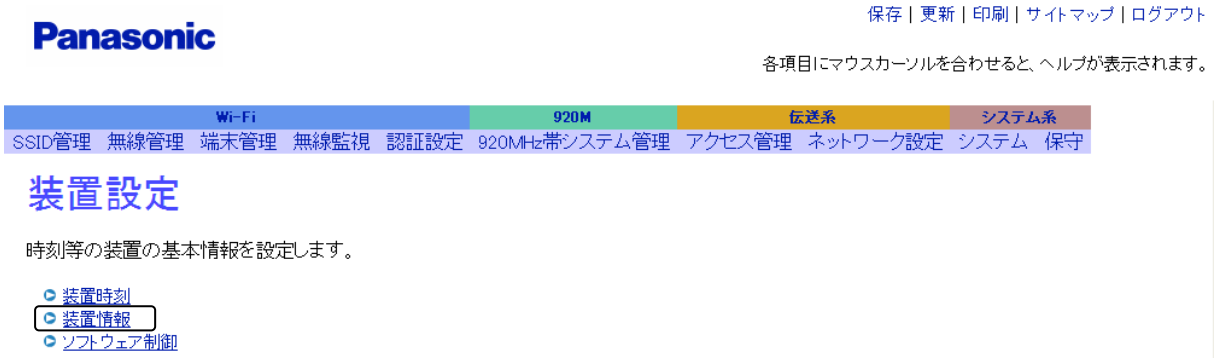


図5.1-8　装置設定

手順7　装置名称を入力します。
（入力は、半角英数字または半角記号（[?]は除く） 0～255 文字以内で行ってください。）
「装置名称（SysName）」は、L2TP 設定の自装置ホスト名となります。

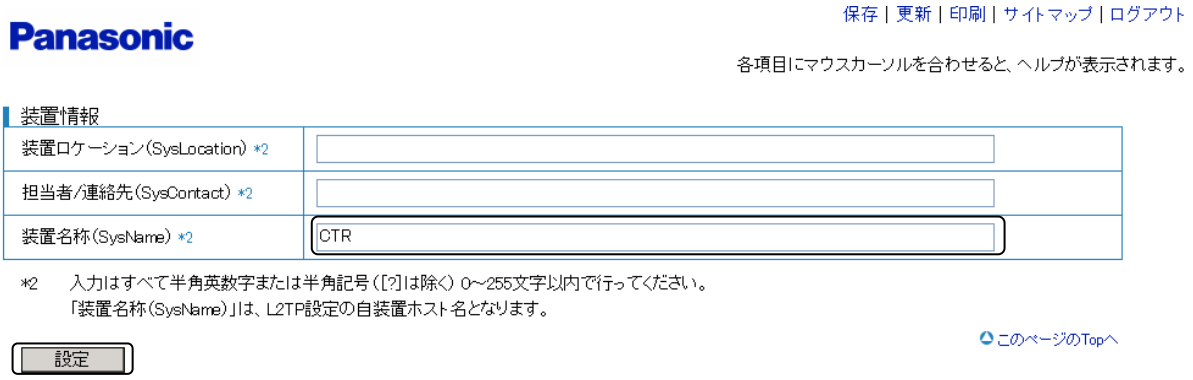


図5.1-9　装置情報

手順8　装置情報下部の〔設定〕をクリックし、設定を反映させます。

◆PPP 設定

手順9　〔ネットワーク設定〕　→　〔PPP 設定〕を選択します。

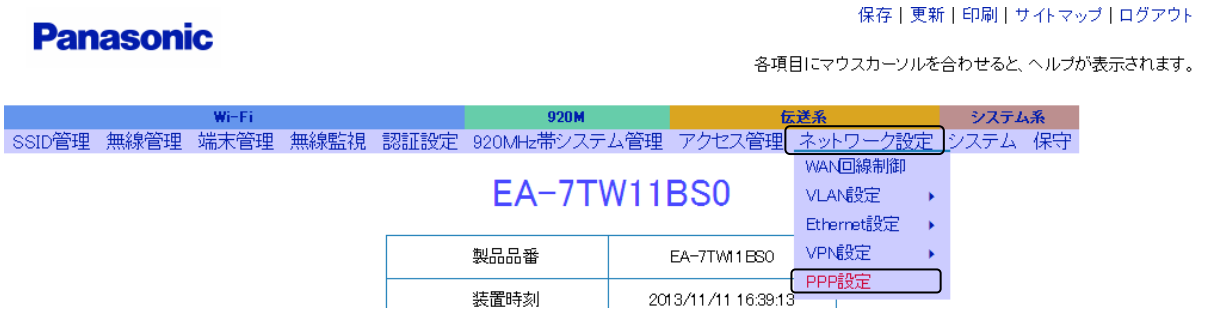


図5.1-10　ネットワーク設定（PPP 設定）

手順 9 は〔PPP 設定〕画面（図 5.1-14）より各種設定を行います。

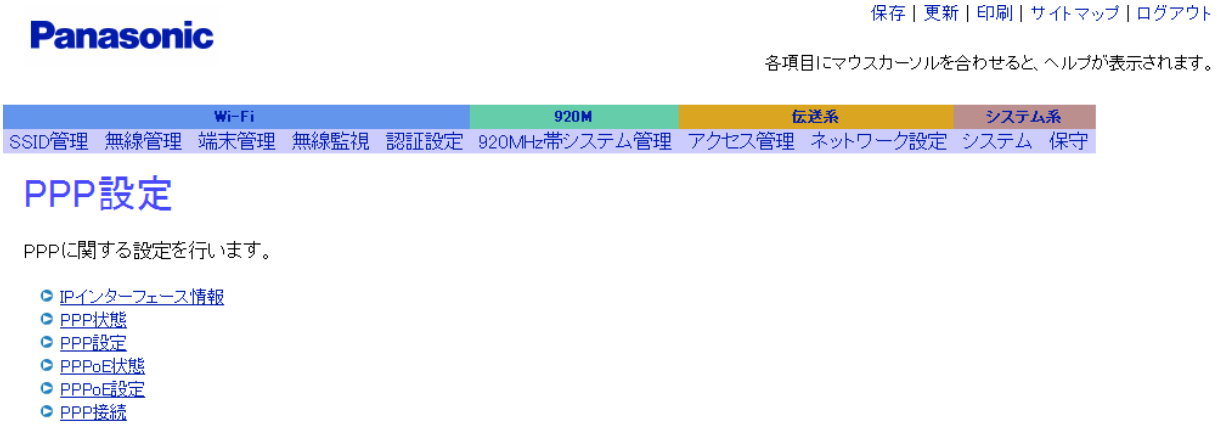


図5.1-11　PPP 設定

手順10　〔PPP 設定〕をクリックし、下記設定を行います。

- 認証方式に〔PAP もしくは CHAP〕を選択
- ログイン名に「Server1234」を入力
- パスワードに「Pass1234」を入力

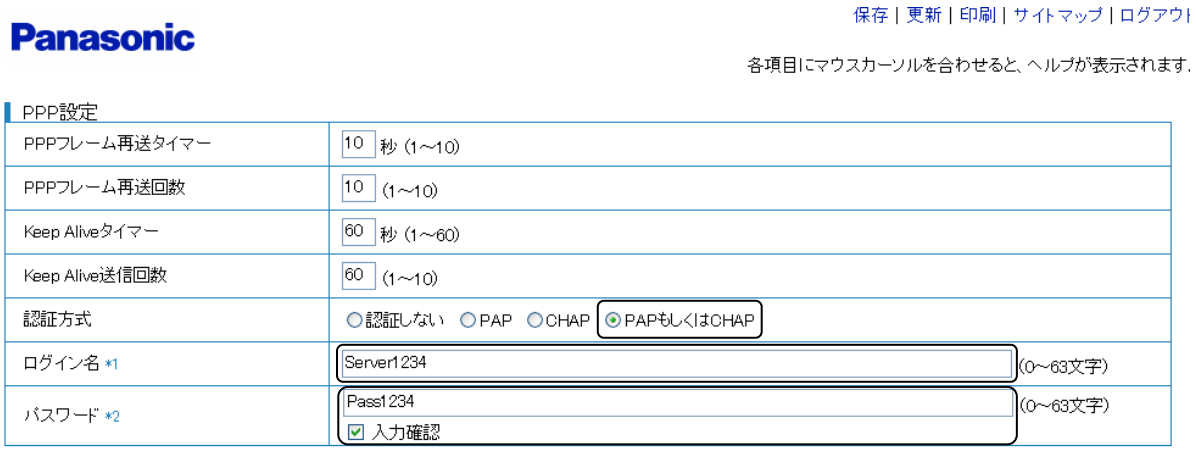


図5.1-12　PPP 設定

手順11　画面最下部の〔設定〕をクリックし、設定を反映させます。

◆L2TP 設定

手順12　〔ネットワーク設定〕　→　〔L2TP 設定〕を選択します。

図5.1-13　ネットワーク設定（L2TP 設定）

手順 13 ～ 手順 15 は〔L2TP 設定〕画面（図 5.1-14）より各種設定を行います。

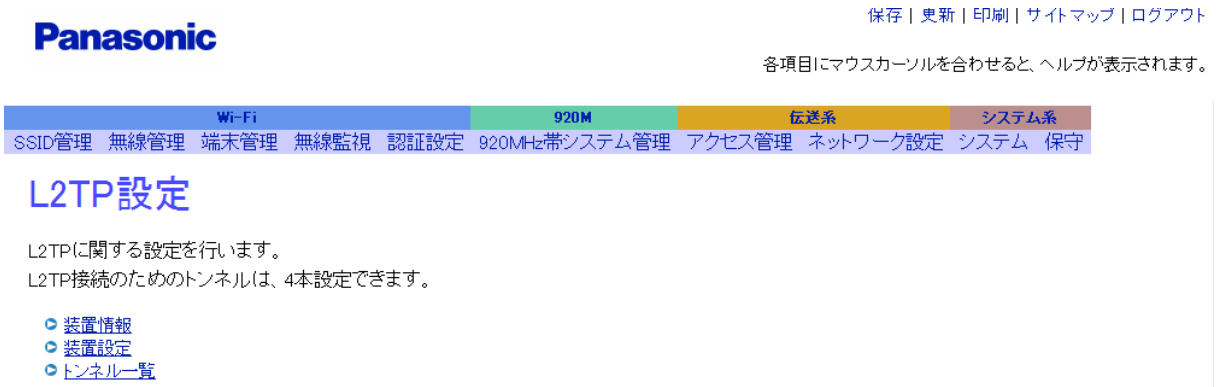


図5.1-14　L2TP 設定

手順13　〔L2TP 設定〕画面（図 5.1-14）の〔装置情報〕をクリックすることで、〔装置設定〕（図 5.1-11）で入力した自装置ホスト名を確認することができます。

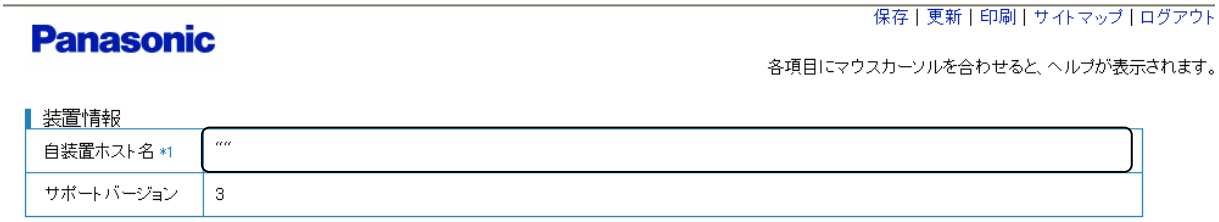


図5.1-15　装置情報

手順14　〔L2TP 設定〕画面（図 5.1-14）の〔装置設定〕をクリックし、ルーターID に「コンセントレータの IP アドレス」を入力し、〔設定〕をクリックして設定を反映させます。

「コンセントレータの IP アドレス」は、PPPoE サーバとの接続が完了した後、〔IP アドレス設定〕
画面（図 5.1-4）で確認してください。

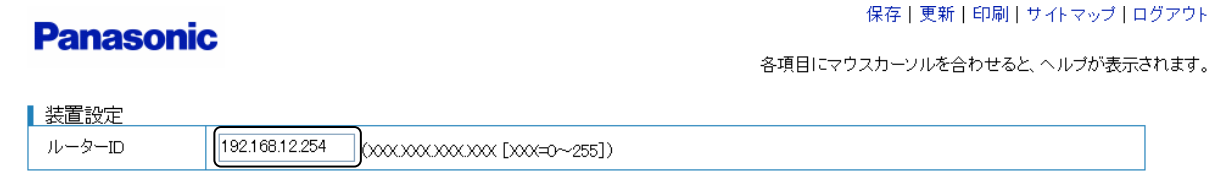


図5.1-16　装置設定

手順15　〔L2TP 設定〕画面（図 5.1-14）の〔トンネル一覧〕をクリックし、トンネル番号 1 の〔編集〕をクリックします。

図5.1-17 トンネル一覧

手順 16 ～ 手順 20 は〔L2TP 編集〕画面（図 5.1-18）より各種設定を行います。

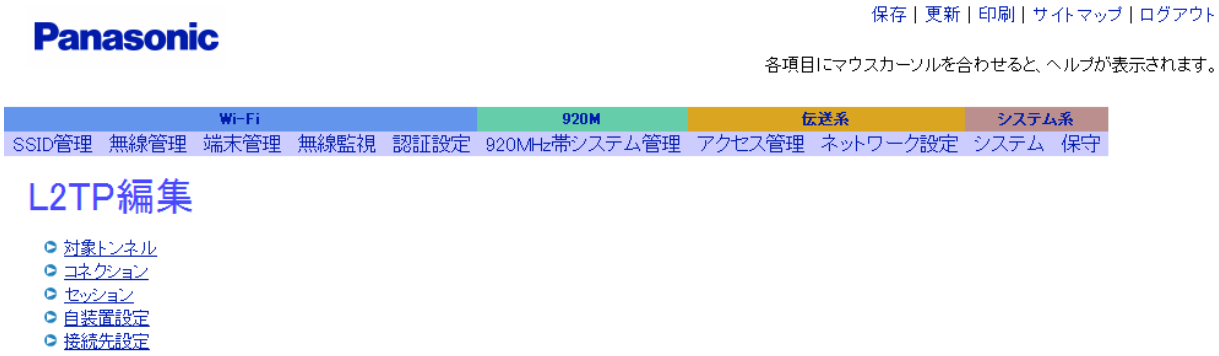


図5.1-18　L2TP 編集

手順16　〔L2TP 編集〕画面（図 5.1-18）の対象トンネルをクリックします。

※ カプセル化方式、UDP ポート番号、ベンダーID については、対向装置と設定を合わせてください。

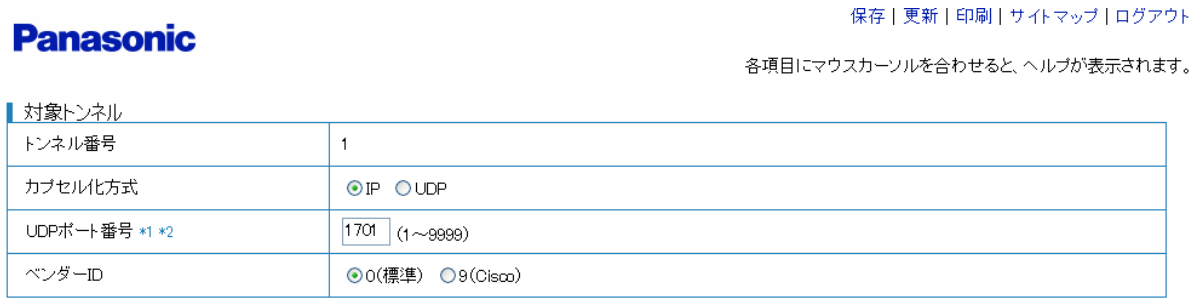


図5.1-19　対象トンネル

手順17　〔L2TP 編集〕画面（図 5.1-18）のコネクションをクリックし、接続開始要求の〔送信〕を選択します。

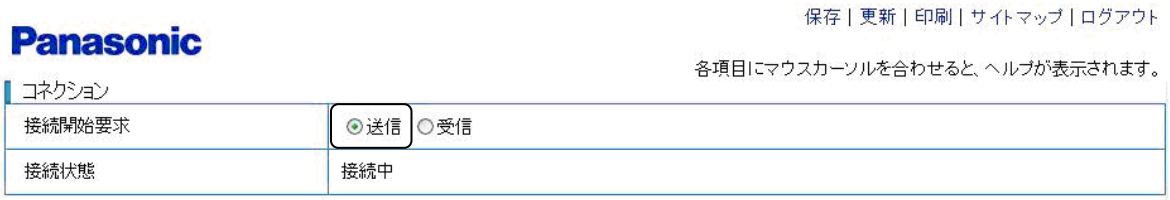


図5.1-20　コネクション

手順18　〔L2TP 編集〕画面（図 5.1-18）の自装置設定をクリックします。

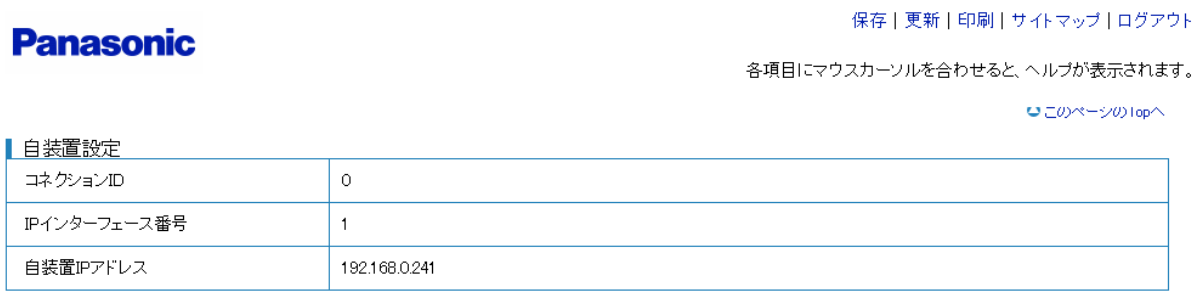


図5.1-21　自装置設定

手順19　〔L2TP 編集〕画面（図 5.1-18）の接続先設定をクリックし、下記内容を入力します。

- 接続先 IP アドレス：192.168.11.252
- 接続先ホスト名：RT
- 接続先ルーターID：192.168.11.252
- 接続用 EndID：1

  ※ 接続用 EndID については、対向装置と設定を合わせてください。

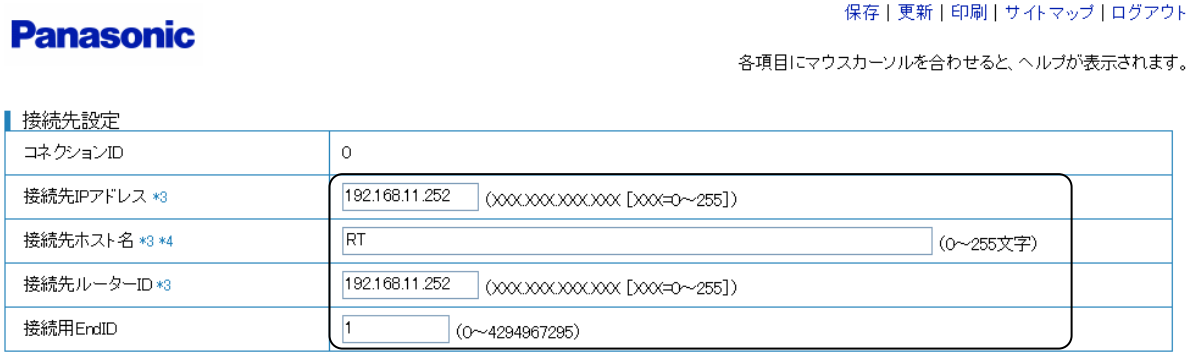


図5.1-22　接続先設定

手順20　画面最下部の〔設定〕をクリックし、設定を反映させます。

5.2　L2TP over IPsec ネットワーク接続での設定

ここでは、L2TP に IPsec を併用することでデータの機密性や完全性を確保した VPN 接続を実現するための基本的な設定方法を説明します。
なお、L2TP 接続先装置の設定については、設置機器の装置マニュアルを別途参照してください。

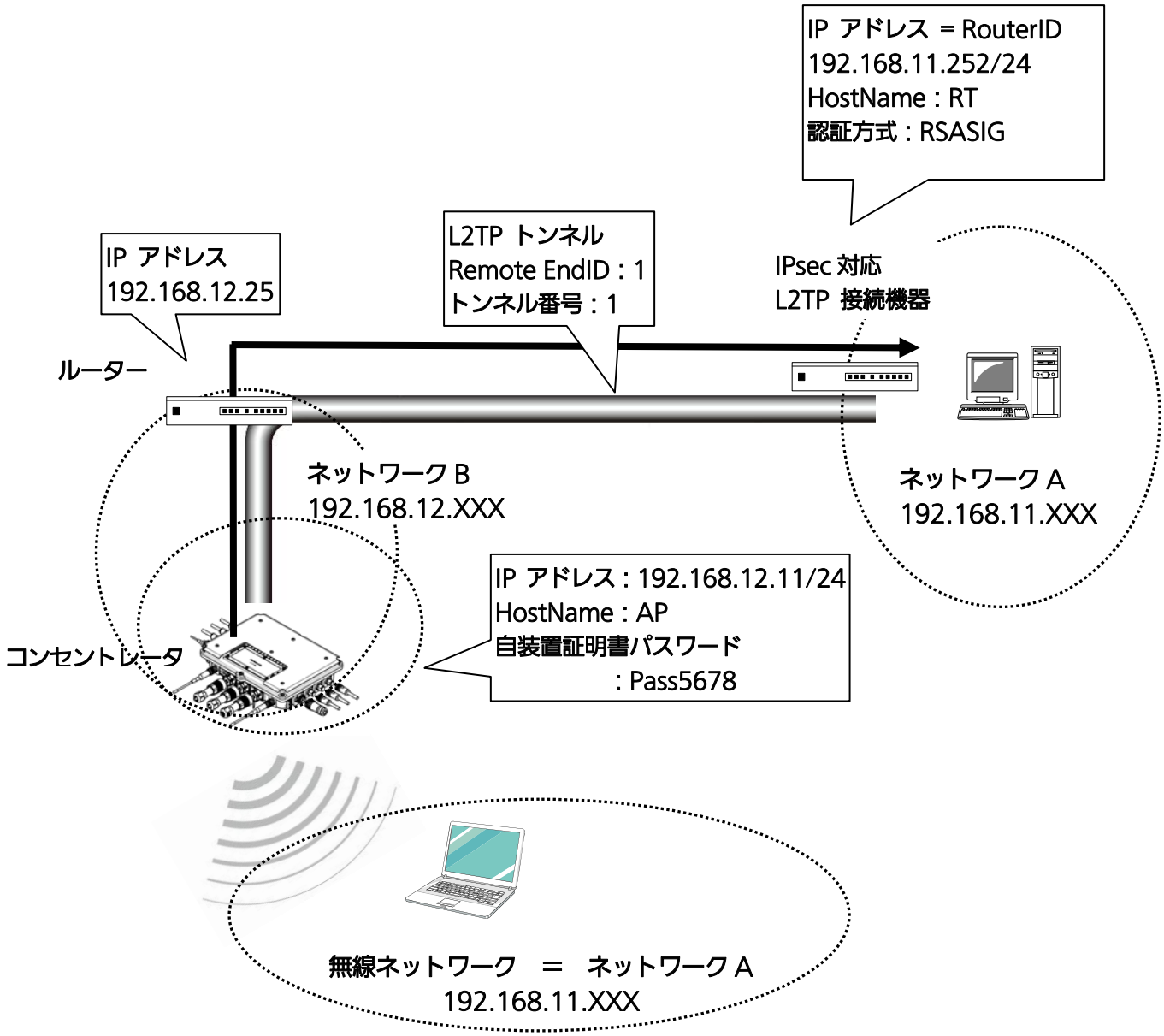


図5.2-1　ネットワーク構成例（L2TP over IPsec）

図 5.2-1（L2TP over IPsec）を構築するための設定は、以下の手順で行います。

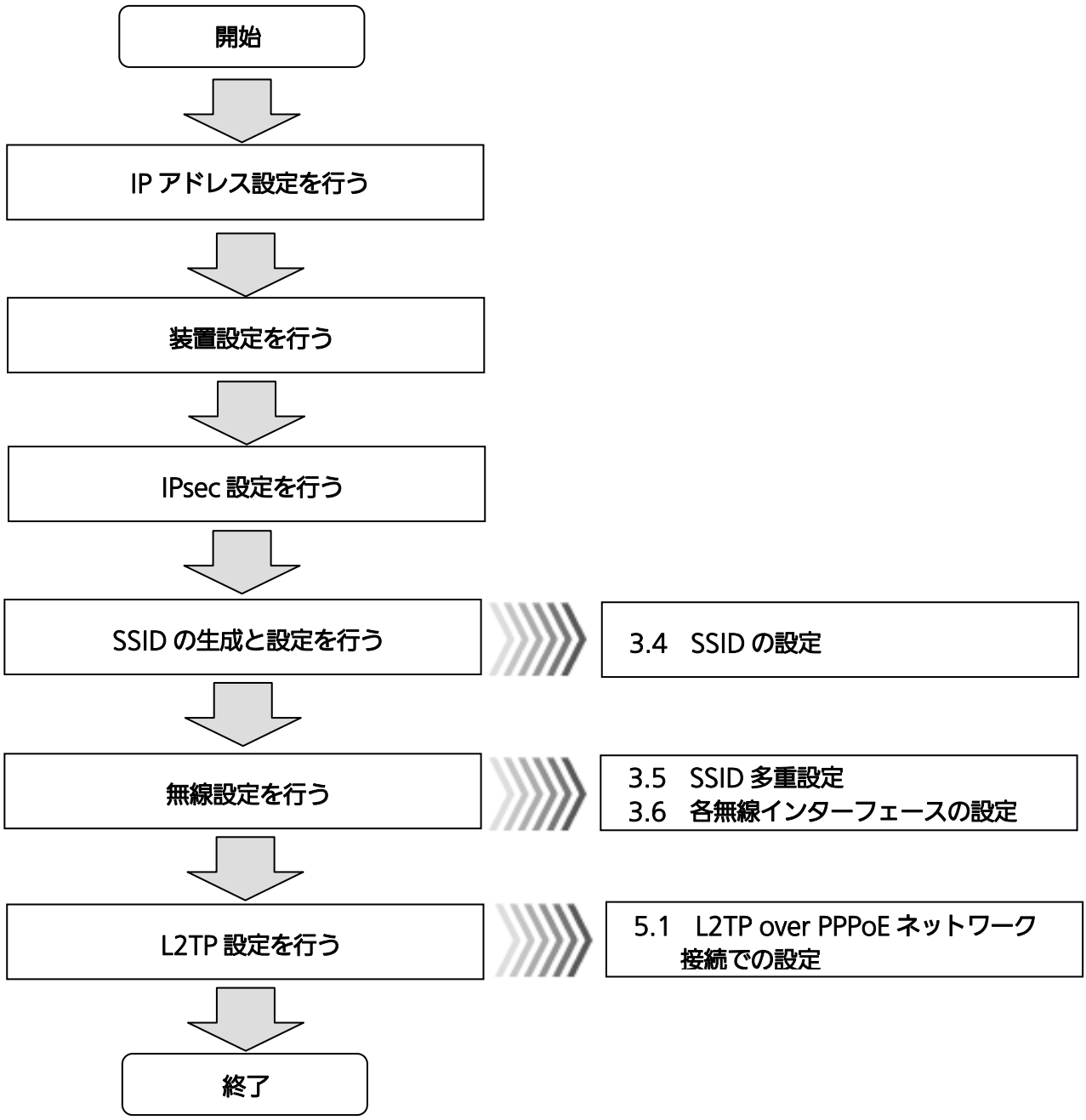


図5.2-2　ネットワーク構成手順（L2TP over IPsec）

設定手順

◆IP アドレス設定

手順1　〔伝送系〕　→　〔システム設定〕　→　〔監視インターフェース設定〕　→　〔IP アドレス設定〕を　選択します。

図5.2-3　メニュー（IP アドレス設定）

手順2　対象となる IP インターフェース 1 番の〔編集〕をクリックします。

図5.2-4　IP アドレス設定

手順 3 ～ 手順 4 は〔IP アドレス編集〕画面（図 5.2-5）より各種設定を行います。

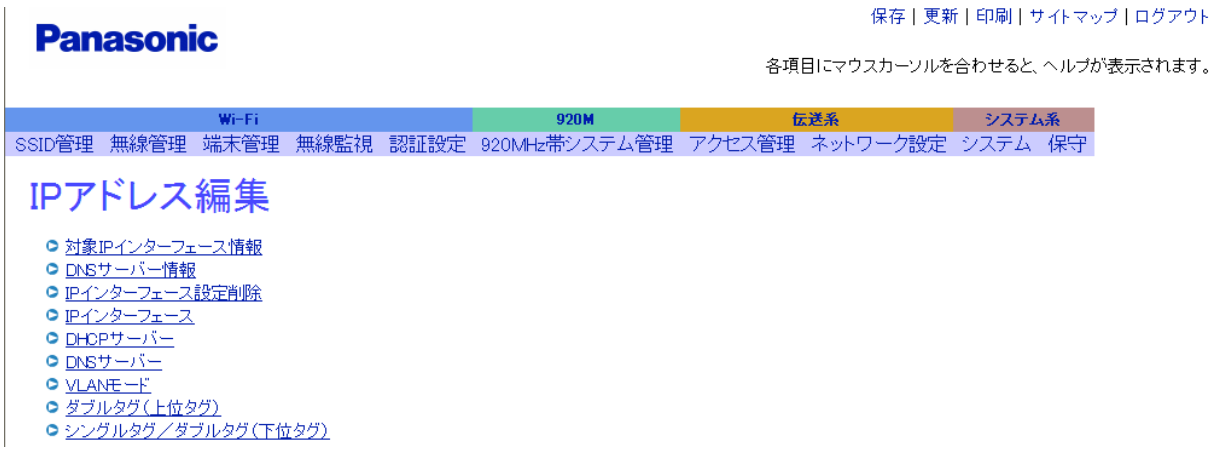


図5.2-5　IP アドレス編集

手順3　〔IP アドレス編集〕画面（図 5.2-5）の〔IP インターフェース〕をクリックし、IP インターフェース 1 番に対して下記設定を行います。

- インターフェースの〔有効〕を選択
- 動作モードの〔Ethernet（固定）〕を選択
- IP アドレスに「192.168.12.11」を入力
- サブネットマスクに「255.255.255.0」を入力
- デフォルトゲートウェイに「192.168.12.254」を入力

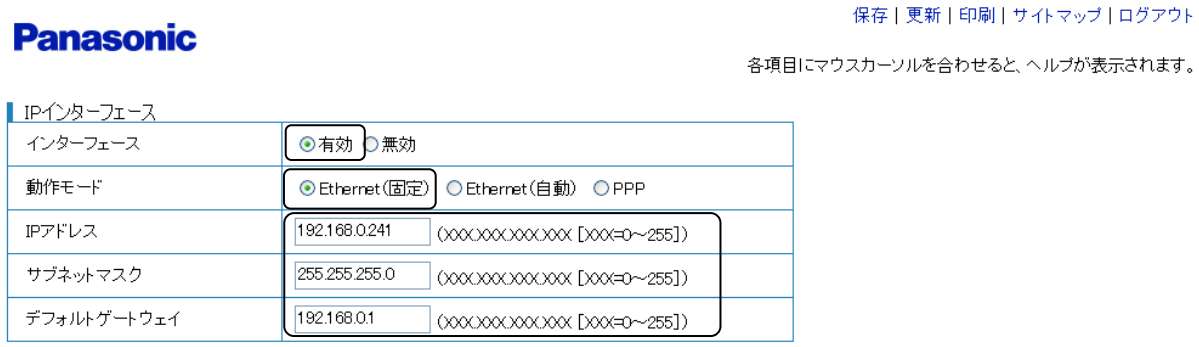


図5.2-6　IP インターフェース設定

手順4　画面最下部の〔設定〕をクリックし、設定を反映させます。

◆装置設定

手順5　〔システム設定〕　→　〔運用設定〕　→　〔装置設定〕を選択します。

図5.2-7　メニュー（装置設定）

手順6　〔装置情報〕をクリックします。

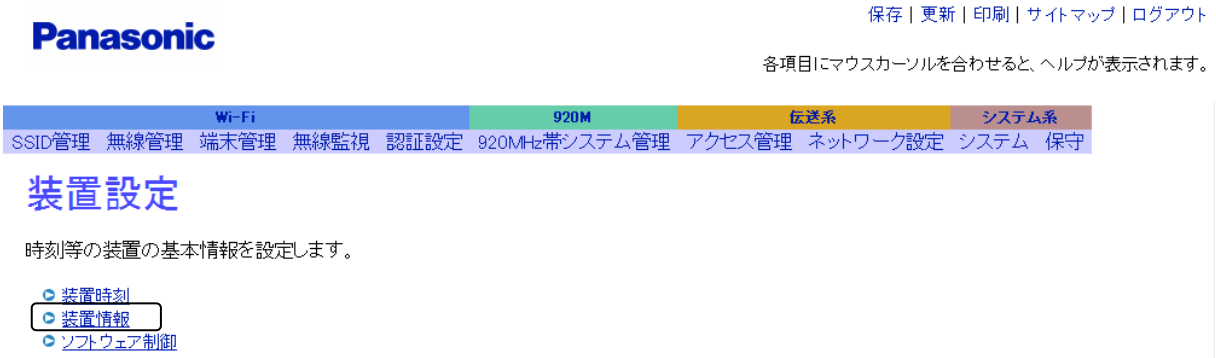


図5.2-8　装置設定

手順7　装置名称を入力します。
（入力は、半角英数字または半角記号（[?]は除く）　0～255 文字以内で行ってください。）
「装置名称（SysName）」は、L2TP 設定の自装置ホスト名となります。

図5.2-9　装置情報

手順8　装置情報下部の〔設定〕をクリックし、設定を反映させます。

◆IPsec 設定

手順9　〔伝送系〕　→　〔ネットワーク設定〕　→　〔IPsec 設定〕を選択します。

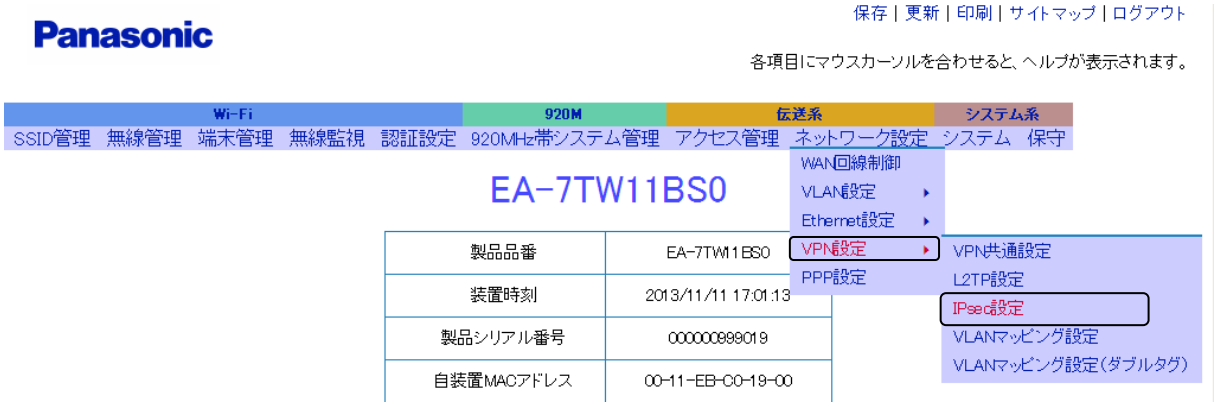


図5.2-10　ネットワーク設定（IPsec 設定）

手順 10 ～ 手順 15 は〔IPsec 設定〕画面（図 5.2-11）より各種設定を行います。

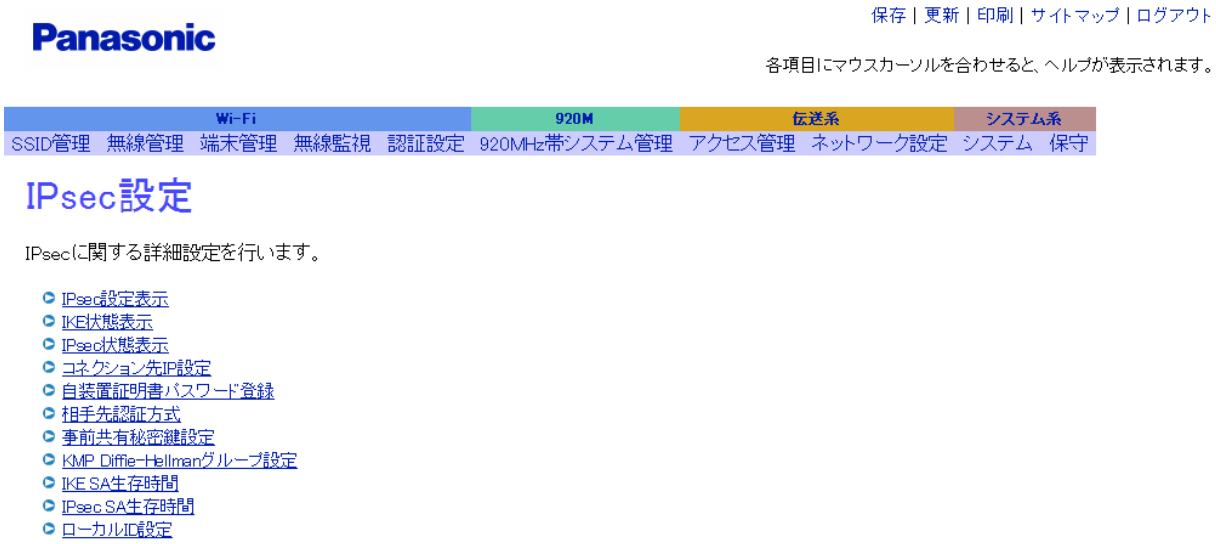


図5.2-11　IPsec 設定

手順10　〔IPsec 設定〕画面（図 5.2-11）の〔コネクション先 IP 設定〕をクリックし、下記内容を設定します。

・ コネクション先 IP アドレスに「192.168.11.252」を入力

図5.2-12　コネクション先 IP 設定

手順11　〔IPsec 設定〕画面（図 5.2-11）の〔自装置証明書パスワード登録〕をクリックし、「Pass5678」を入力します。

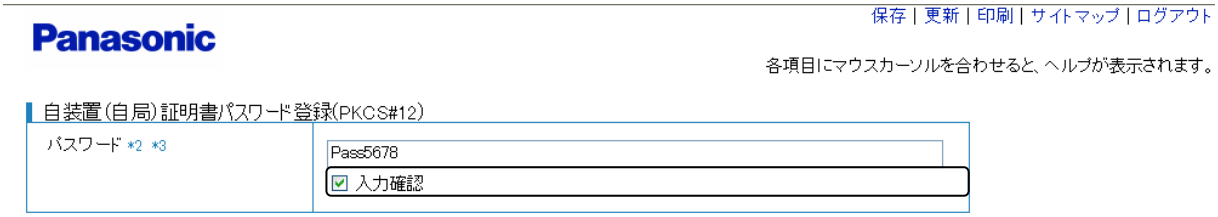


図5.2-13　自装置（自局）証明書パスワード登録(PKCS#12)

手順12　〔IPsec 設定〕画面（図 5.2-11）の〔相手先認証方式〕をクリックし、〔RSASIG〕を選択します。

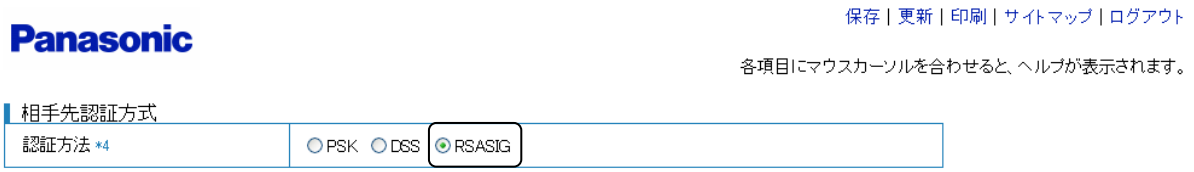


図5.2-14　相手先認証方式

手順13　〔IPsec 設定〕画面（図 5.2-11）の〔ローカル ID 設定〕をクリックし、〔IP アドレス、または、公開鍵証明書のサブジェクト〕を選択します。

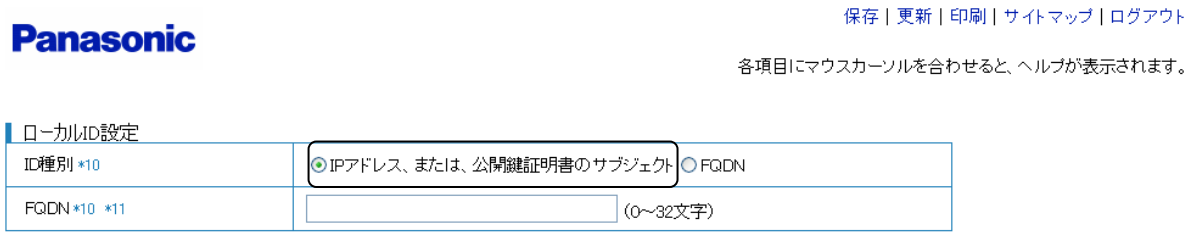


図5.2-15　ローカル ID 設定

手順14　画面最下部の〔設定〕をクリックし、設定を反映させます。

以下、「5.1　L2TP over PPPoE ネットワーク接続での設定」の手順 12 ～ 手順 20（◆L2TP 設定）をご参照ください。

重要	■ IPsec を認証方式＝DSS、RSASIG で接続する場合は、あらかじめ各種証明書を FTP または TFTP でコンセントレータに put しておく必要があります。 ■ DSS、RSASIG では、対向装置とコンセントレータの時刻がずれていた場合、接続が失敗するおそれもありますのでご注意ください。

第６章　920MHz帯 ネットワーク

920MHz帯 ネットワークについて、説明します。

6.1　920MHz 帯ネットワーク概要

6.1.1　特長

920MHz 帯ネットワークを用いたマルチアクセス コンセントレータは、各種センサから出力されたデータを920MHz帯 通信ユニットが取得し、920MHz帯特定小電力無線を用いてマルチアクセス コンセントレータへ送信します。マルチアクセス コンセントレータは、収集された各種センサデータを TRAP によりセンサ情報収集アプリケーションサーバへ送信することができます。
マルチアクセス コンセントレータは、920MHz 帯 通信ユニットを通じて、異なる種別のセンサを混在して収容することができます。

6.1.2　構成例

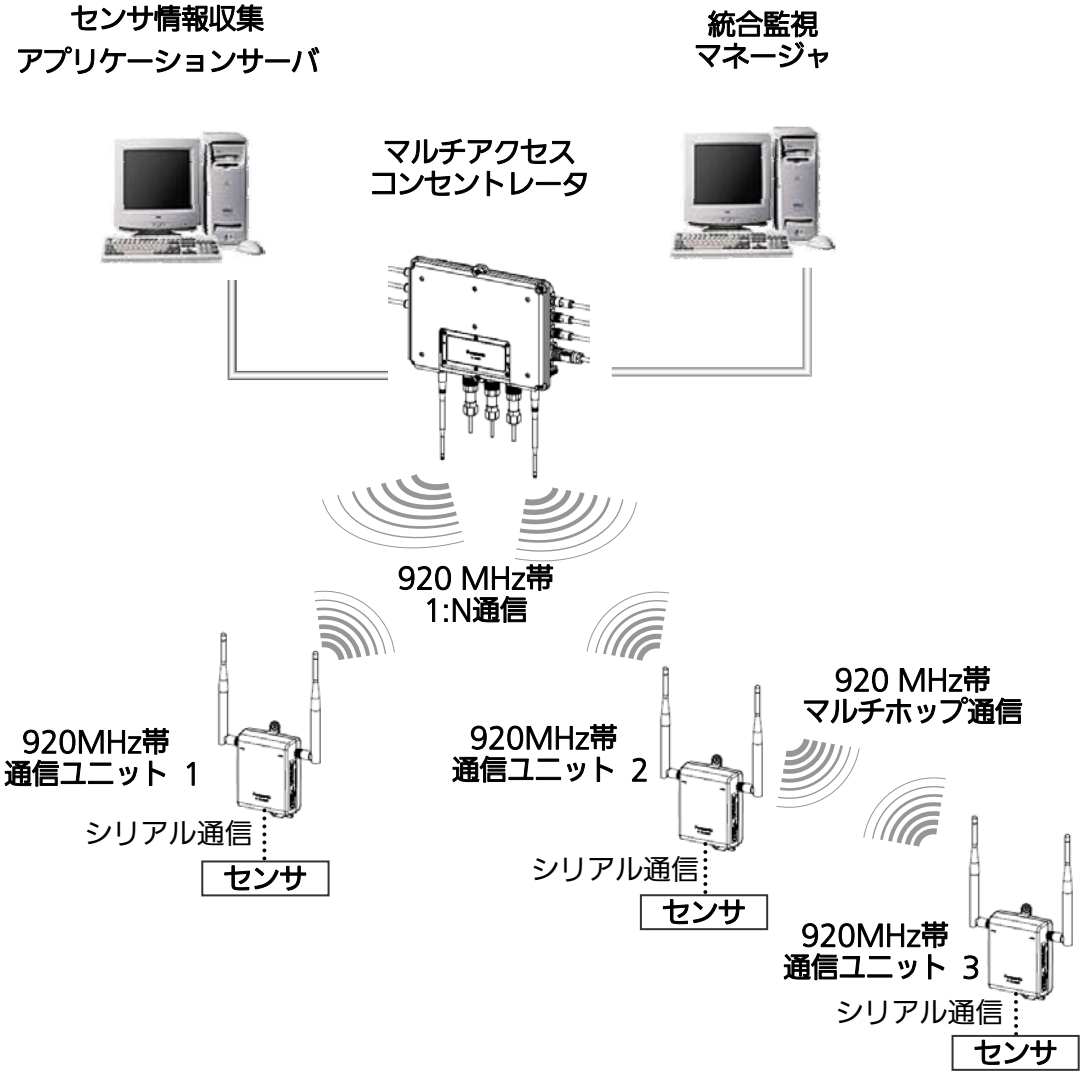


図6.1-1　構成例

マルチアクセス コンセントレータ、および、920MHz 帯 通信ユニットの基本的な設定は、以下の手順で行います。

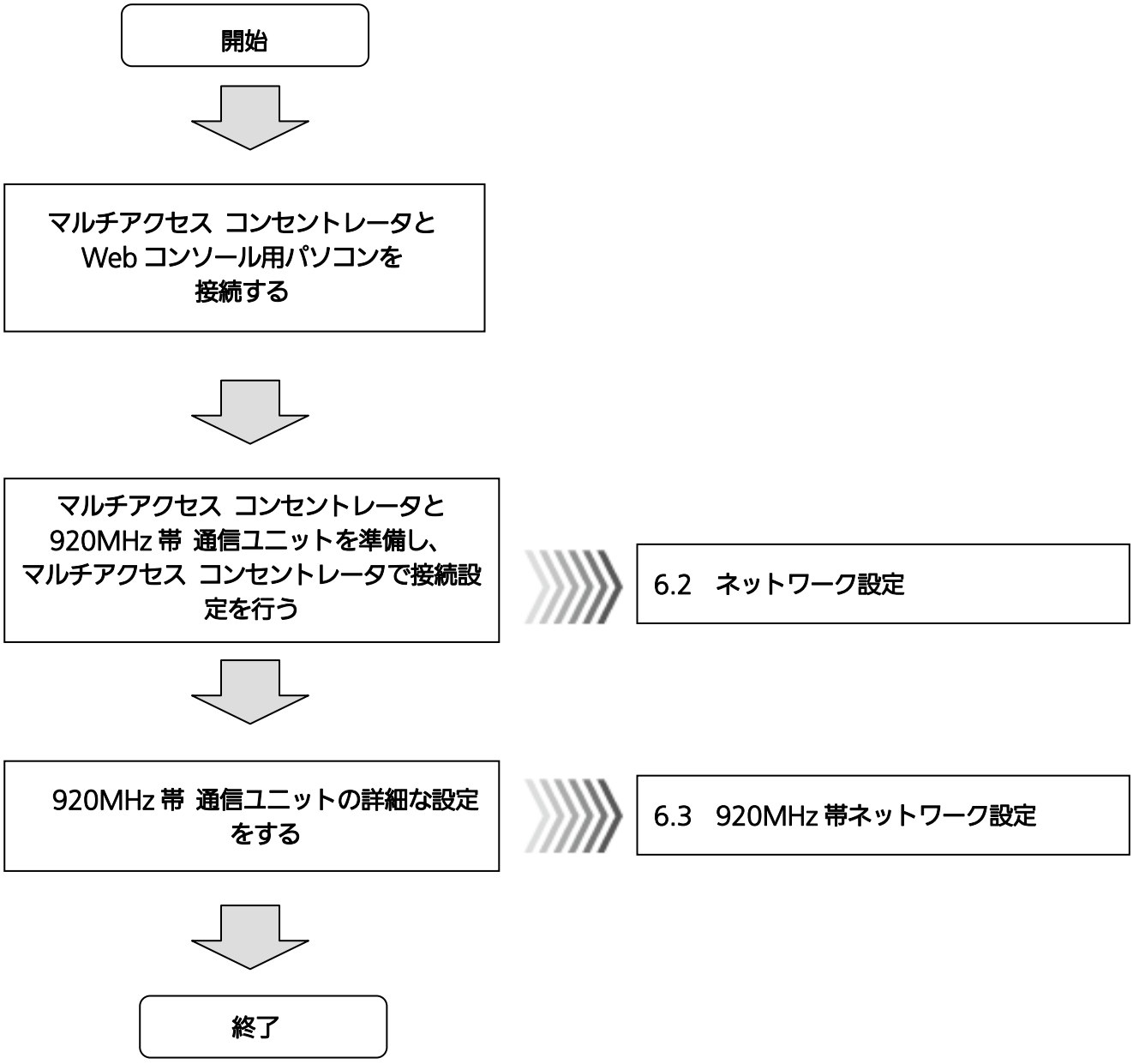


図6.1-2　920MHz 帯ネットワークの設定手順

6.2　ネットワーク設定

920MHz 帯ネットワークを構築するための基本的な設定方法を説明します。
コンセントレータでは、920MHz 帯ネットワークを構築するにあたり、下記の順番で設定を行います。

6.2.1　IP アドレス設定

各装置を接続するため、マルチアクセス コンセントレータにて IP アドレスの設定を行います。

■IP アドレスの設定

設定手順

手順1　〔システム系〕　→　〔監視インターフェース設定〕　→　〔IP アドレス設定〕を選択します。

図6.2-1 メニュー(IP アドレス設定)

手順2　対象となる IP アドレスの〔編集〕をクリックします。

図6.2-2　IP アドレス設定一覧

手順3　IP インターフェースをクリックします。

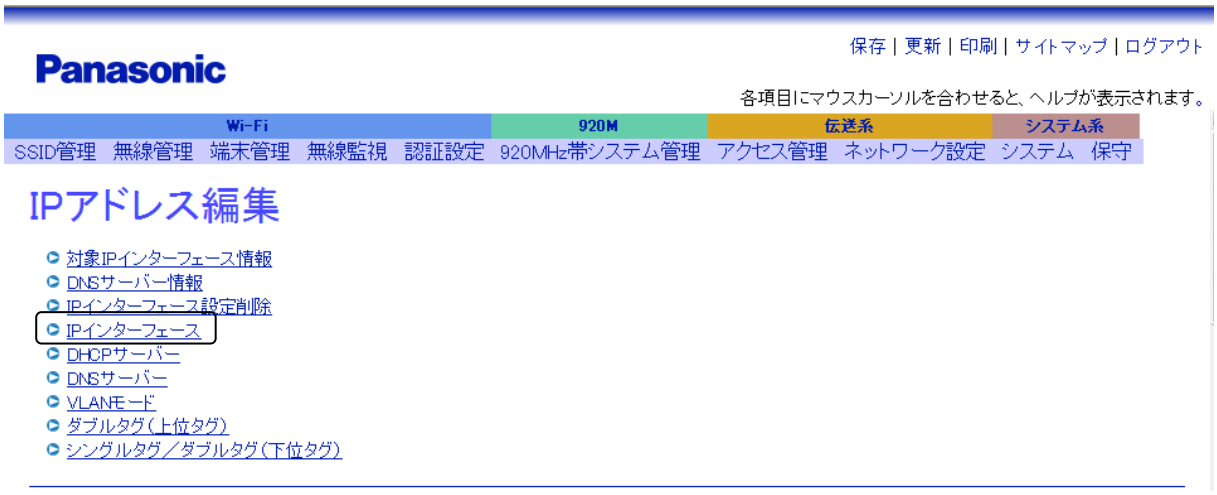


図6.2-3　IP アドレス編集

手順4　IP インターフェースの設定をします。

- インターフェースを有効
- 動作モードは Ethernet(固定)を選択
- PPP 動作モードは Ethernet を選択
- IP アドレスに「192.168.100.254」を入力
- サブネットマスクに「255.255.255.0」を入力
- デフォルトゲートウェイに「192.168.100.0」を入力

図6.2-4　IP インターフェース編集

手順5　画面最下部の〔設定〕をクリックし、設定を反映させます。

6.2.2　SNMP 設定

マルチアクセス コンセントレータにて、制御元となる SNMP の設定を行います。

■SNMP の設定

設定手順

手順1　〔システム系〕 → 〔システム〕 → 〔監視設定〕 → 〔SNMP 設定〕を選択します。

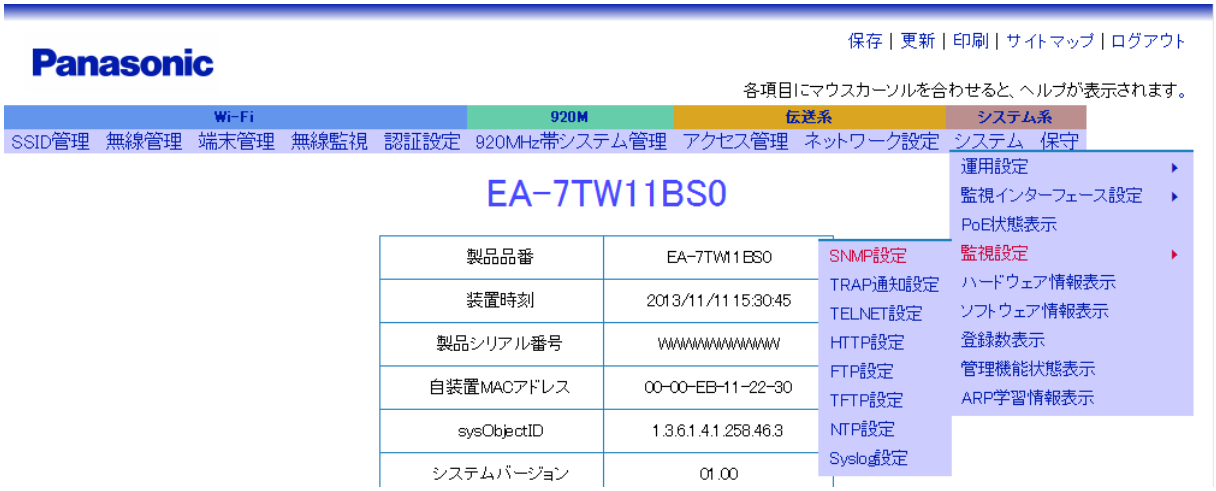


図6.2-5　メニュー（SNMP 設定）

手順2　SNMP のアクセス許可するため、〔アクセス設定〕の〔許可〕を選択クリックし、〔設定〕をクリックします。

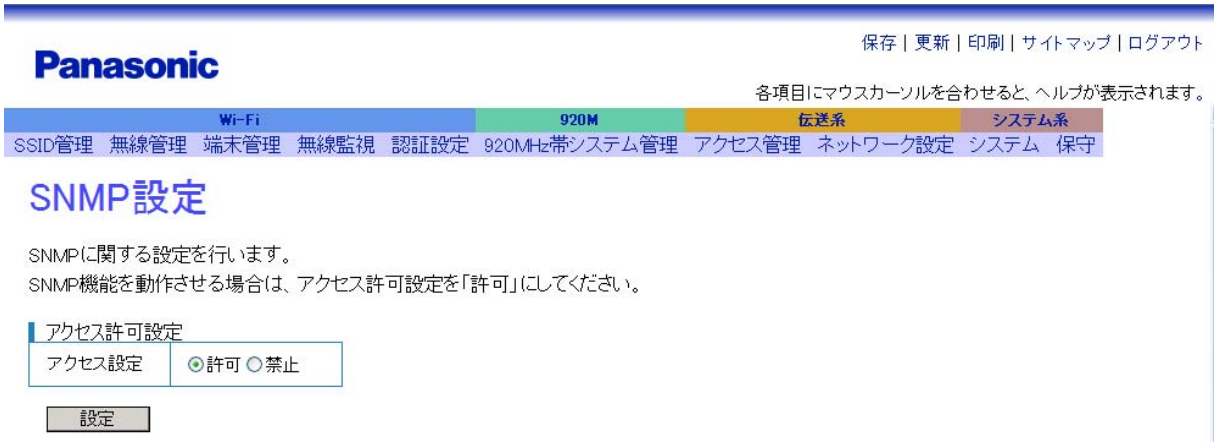


図6.2-6　SNMP 設定

手順3　対象となる SNMP 番号の SNMP コミュニティー〔編集〕をクリックし、編集を行います。

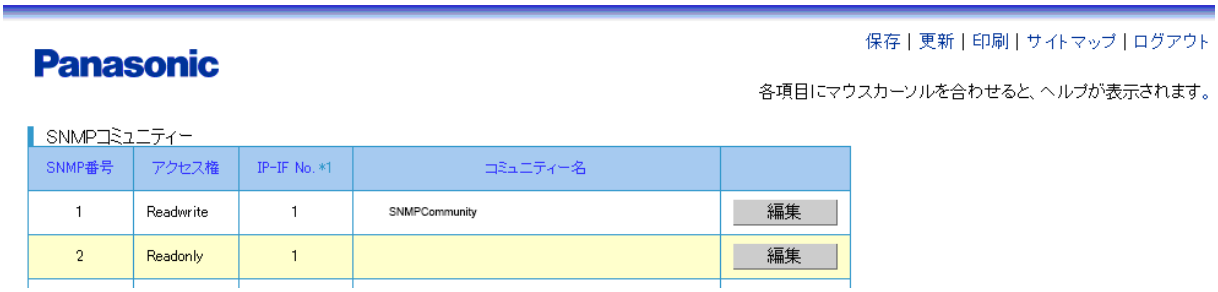


図6.2-7　SNMP コミュニティー

手順4　SNMP の編集を行います。

- アクセス権を ReadWrite を選択
- IP インターフェース番号〔1〕を選択
- コミュニティー名は「SNMPCommunity」を入力

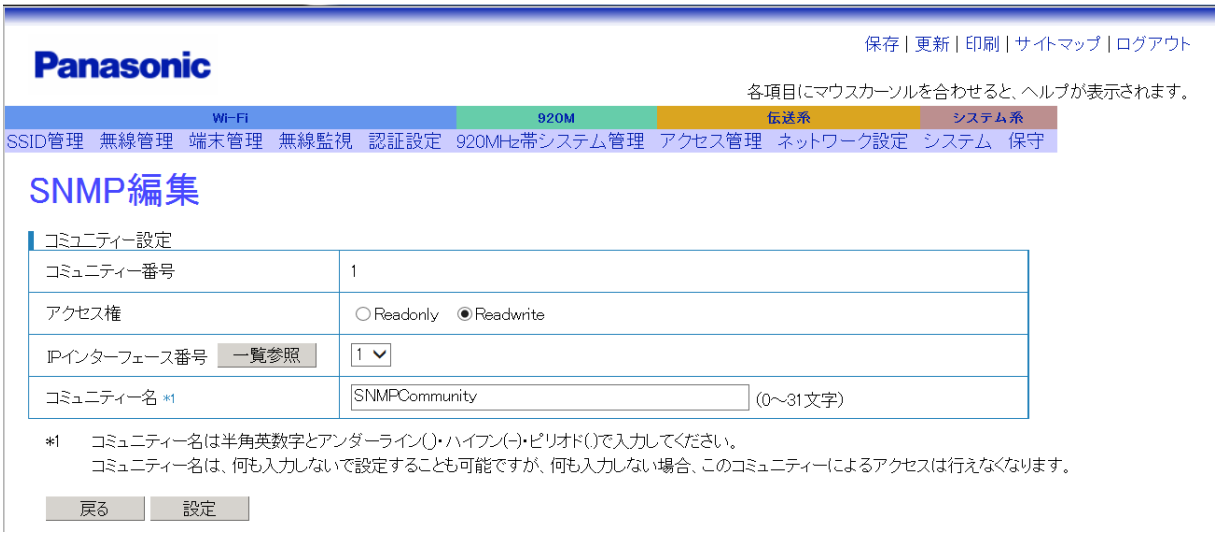


図6.2-8　SNMP 編集

手順5　画面最下部の〔設定〕をクリックし、設定を反映させます。

6.2.3　TRAP 通知設定

マルチアクセス コンセントレータにて、制御先となる TRAP 通知の設定を行います。

■SNMP の設定

設定手順

手順1　〔システム系〕 → 〔システム〕 → 〔監視設定〕 → 〔TRAP 通知設定〕を選択します。

図6.2-9　メニュー(TRAP 通知設定)

手順2　対象となる TRAP 番号の〔編集〕をクリックします。

図6.2-10　TRAP 通知設定

手順3　対象となるTRAP番号の〔編集〕をクリックします。

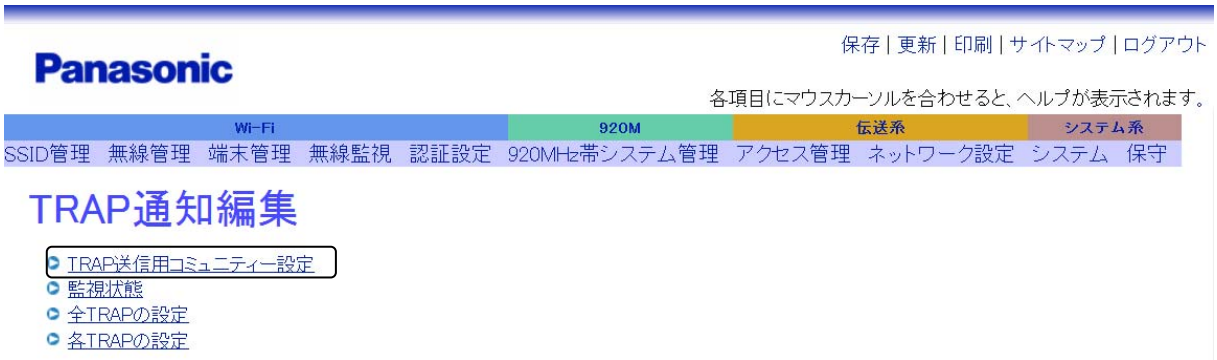


図6.2-11　TRAP通知編集

手順4　TRAP送信用コミュニティーの設定をします。

- IPインターフェース番号〔1〕を選択
- 通知先IPアドレスは「192.168.100.1」を入力
- TRAPバージョンはTrapV1を選択
- コミュニティー名は「TRAPCommunity」を入力

図6.2-12　TRAP送信用コミュニティー設定

手順6　全TRAPの設定をします。

- 全TRAPの通知は有効を選択

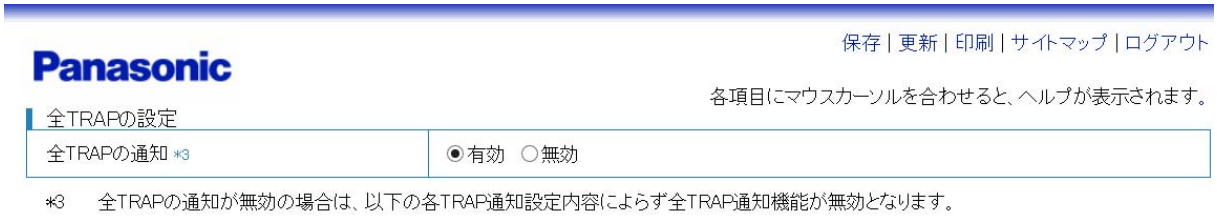


図6.2-13　全TRAPの設定

手順7　画面最下部の〔設定〕をクリックし、設定を反映させます。

6.2.4　センサデータ制御元設定

センサの発行元の設定であるセンサデータ制御元設定を行います。

■センサデータ制御元の設定

設定手順

手順1　〔920M〕　→　〔920MHz 帯ネットワーク設定〕　→　〔センサデータ制御元設定〕を選択します。

図6.2-14　メニュー(センサデータ制御元設定)

手順2　対象となるセンサデータ制御元設定の〔編集〕をクリックします。

図6.2-15　センサデータ制御元設定一覧

手順3　センサデータ制御元の編集をします

- アクセス権は ReadWrite を選択
- IP インターフェース番号は 1（6.2.1 で設定した IP インターフェース）を選択。
- コミュニティー名に「SNMPCommunity」を入力

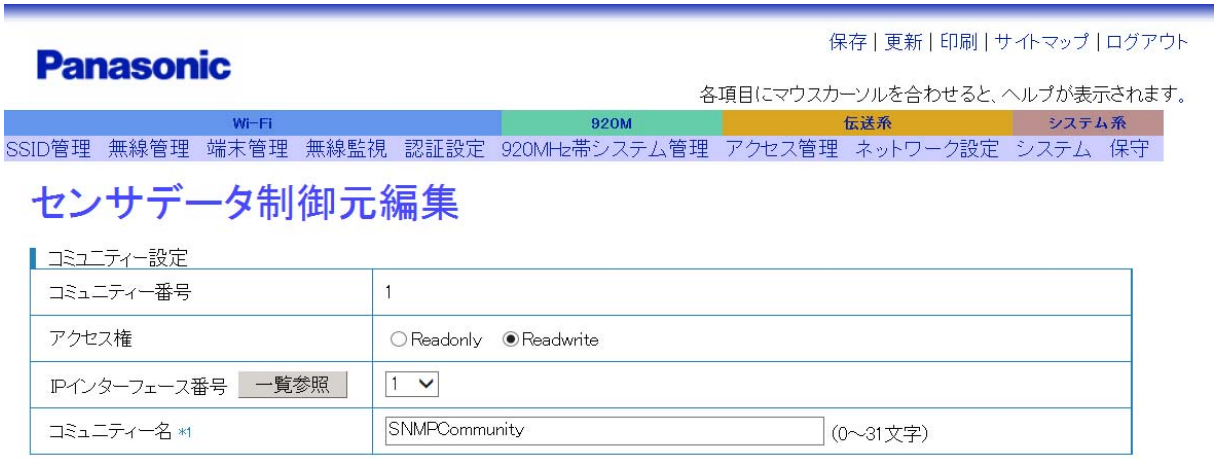


図6.2-16　センサデータ制御元編集

手順4　画面最下部の〔設定〕をクリックし、設定を反映させます。

6.2.5　センサデータ制通知先設定

センサの通知先の設定であるセンサデータ通知先設定を行います。

■センサデータ通知先の設定

設定手順

手順1　〔920M〕　→　〔920MHz 帯ネットワーク設定〕　→　〔センサデータ通知先設定〕を選択します。

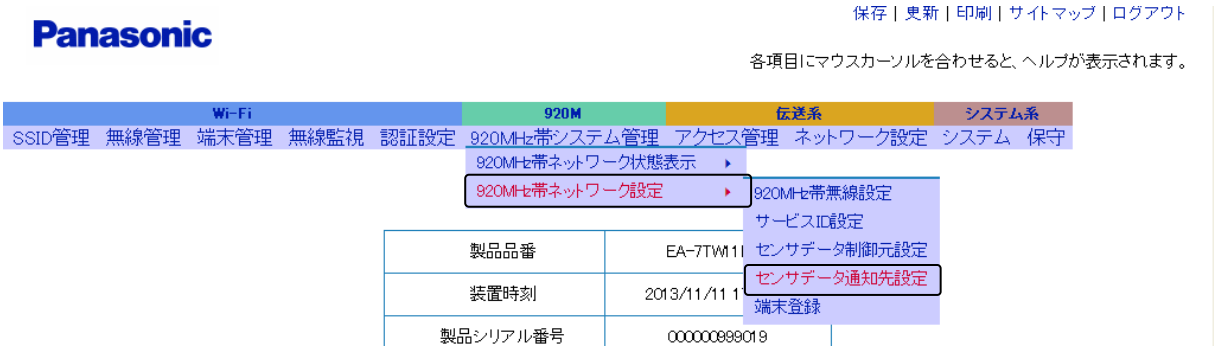


図6.2-17　メニュー(センサデータ通知先設定)

手順2　対象となるセンサデータ通知先設定の〔編集〕をクリックします。

図6.2-18　センサデータ通知先設定

手順3　対象となる TRAP 送信用コミュニティーの設定を行います。

- IP インターフェース番号は 1 を選択します。
- 通知先アドレスに「192.168.200.2」を入力。
- TRAP バージョンは〔TrapV1〕を選択。
- TRAP 送信用コミュニティー名に「TRAPCommunity」を入力します。

図6.2-19　TRAP 送信用コミュニティー設定

手順4　TRAP の設定を行います。

- pPartSensorData は通知を選択。

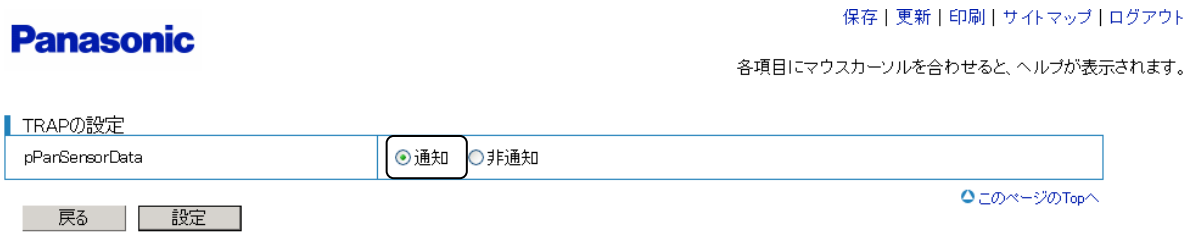


図6.2-20　TRAP の設定

手順5　画面最下部の〔設定〕をクリックし、設定を反映させます。

6.3　920MHz 帯ネットワーク設定

920MHz 帯ネットワークを構築するための基本的な設定方法を説明します。

6.3.1　サービス ID 設定

920MHz 帯 通信ユニットの端末登録の設定を行い、サービス ID に紐付けを行います。

設定手順

手順1　〔920M〕　→　〔920MHz 帯ネットワーク設定〕　→　〔サービス ID 設定〕を選択します。

図6.3-1　メニュー（サービス ID 設定）

手順2　サービス ID 設定を行います。

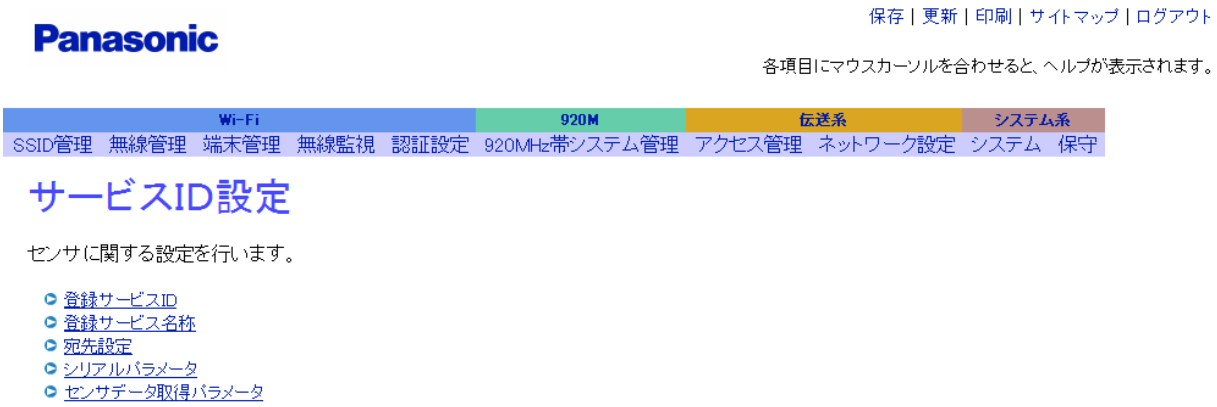


図6.3-2　サービス ID 設定

手順3　登録サービス ID の設定を行います。

・ サービス ID は任意ですが、ここでは「2」を入力します。

図6.3-3　登録サービス ID 設定

手順4　登録サービス名称の設定を行います。

・ サービス名称は任意ですが、「Service02」を入力します。

図6.3-4　登録サービス名称設定

手順5　宛先設定を行います。

・ TRAP 番号は 6.2.5 で設定をした「1」を入力します。

図6.3-5　宛先設定

手順6　シリアルパラメーターの設定を行います。

- ボーレートは 4800 を選択します。
- データビットは〔8bit〕を選択。
- パリティは〔無し〕を選択。
- ストップビットは〔1bit〕を選択。
- フロー制御(ハードウェアフロー)は〔無効〕を選択。

図6.3-6　シリアルパラメーター設定

手順7　センサデータ取得パラメーターの設定を行います。

- データ判定間隔は「1」を入力します。
- データの間引きは〔無効〕を選択。

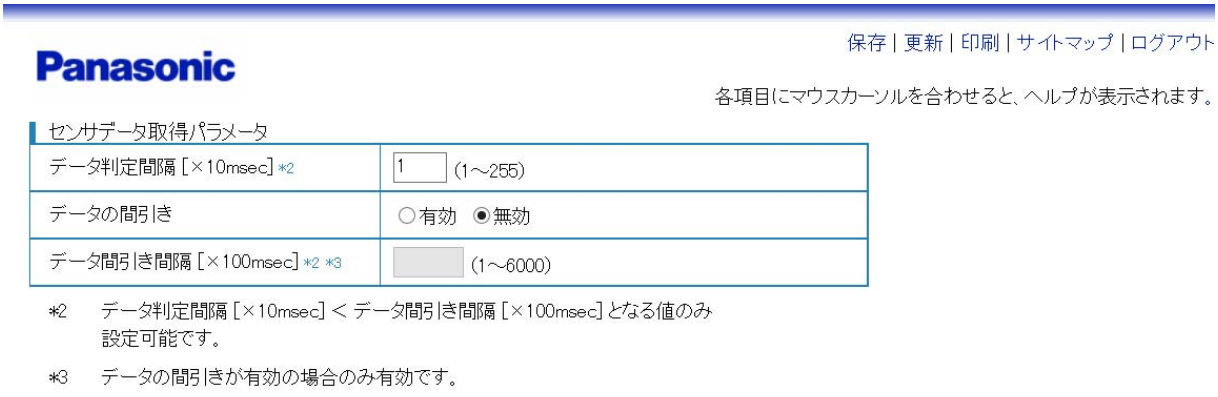


図6.3-7　センサデータ取得パラメーター設定

手順8　画面最下部の〔設定〕をクリックし、設定を反映させます。

6.3.2　端末登録

設定手順

手順1　〔920M〕　→　〔920MHz 帯ネットワーク設定〕　→　〔端末登録〕を選択します。

図6.3-8　メニュー(端末登録)

手順2　対象となる端末登録を行います。

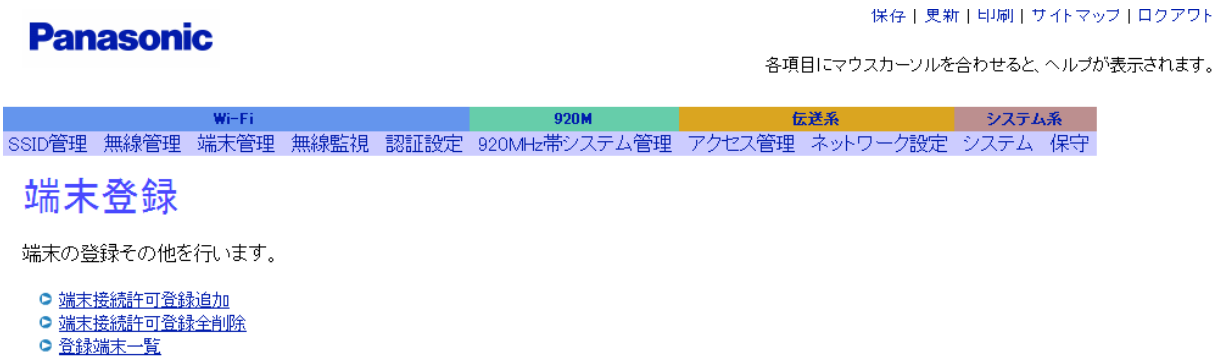


図6.3-9　端末登録

手順3　端末接続許可登録追加を行います。

なお、センサを接続しない 920MHz 帯 通信ユニットを登録する場合は、サービス ID には「0」を入力してください。

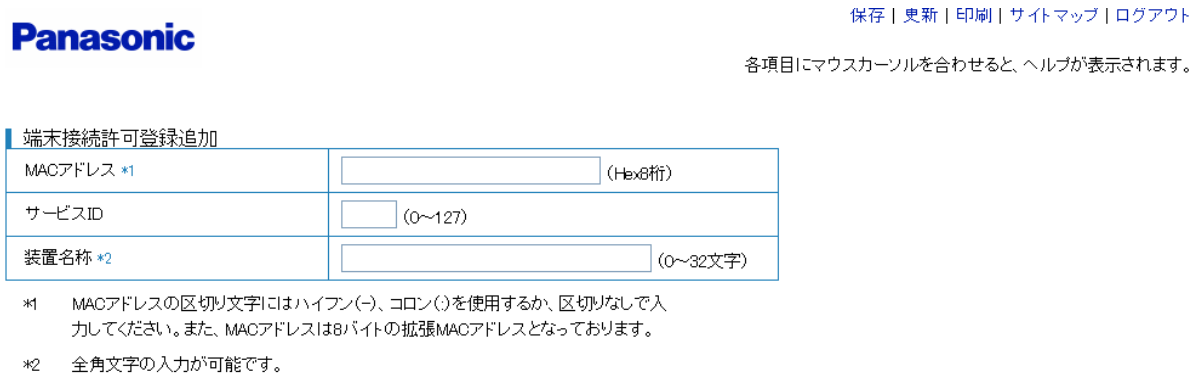


図6.3-10　端末接続許可登録追加

6.3.3　920MHz 帯無線設定

920MHz 帯の無線設定の設定を行います。

設定手順

手順1　〔920M〕　→　〔920MHz 帯ネットワーク設定〕　→　〔920MHz 帯無線設定〕を選択します。

図6.3-11　メニュー(920MHz 帯無線設定)

手順2　対象となる 920MHz 無線設定を行います。

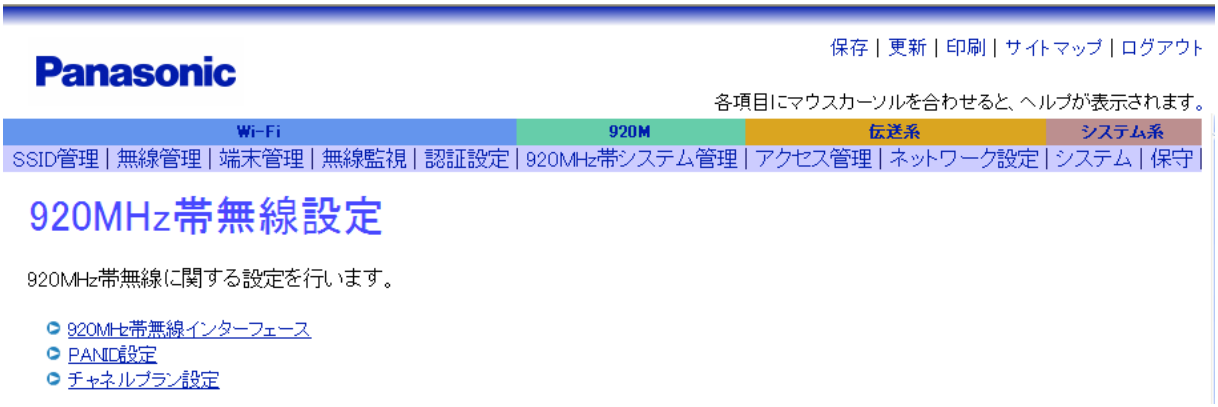


図6.3-12　920MHz 帯無線設定

手順3　920MHz 帯無線インターフェースの設定を行います。

・ 920MHz 帯無線インターフェースは〔有効〕を選択。

図6.3-13　920MHz 帯無線インターフェース

手順4　PAN-ID の設定を行います。

・ PAN-ID は任意の数字です。ここでは「3」を入力。

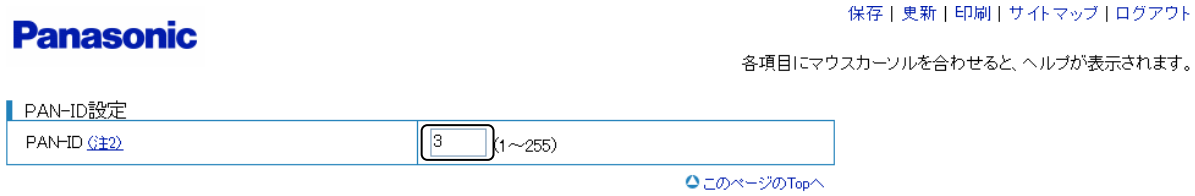


図6.3-14　PAN-ID 設定

手順5　チャネルプランの設定を行います。

・ チャネルプランは任意の数字です。ここでは〔2〕を選択。

図6.3-15　チャネルプラン設定

手順6　画面最下部の〔設定〕をクリックし、設定を反映させます。

第 7 章　保守

コンセントレータの保守機能（ログ機能、アップロード・ダウンロード、装置リセットなど）について、説明します。

7.1　設定データのバックアップと読み込み

7.1.1　設定データのバックアップ

コンセントレータの設定データをバックアップする方法は、FTP コマンドを使用する方法、WEB コンソールでファイルコピーを使用する方法、CLI コンソールでコマンドを実行する方法があります。ここでは、FTP コマンドを使用して、コンセントレータに接続している PC に設定ファイルをバックアップする方法を紹介します。一部の設定は設定データでバックアップできないため、全設定をバックアップしたい場合は、全設定一括バックアップをご利用ください。

操作手順

手順1　〔伝送系〕 → 〔システム設定〕 → 〔運用設定〕 → 〔ファイル名設定〕を選択します。

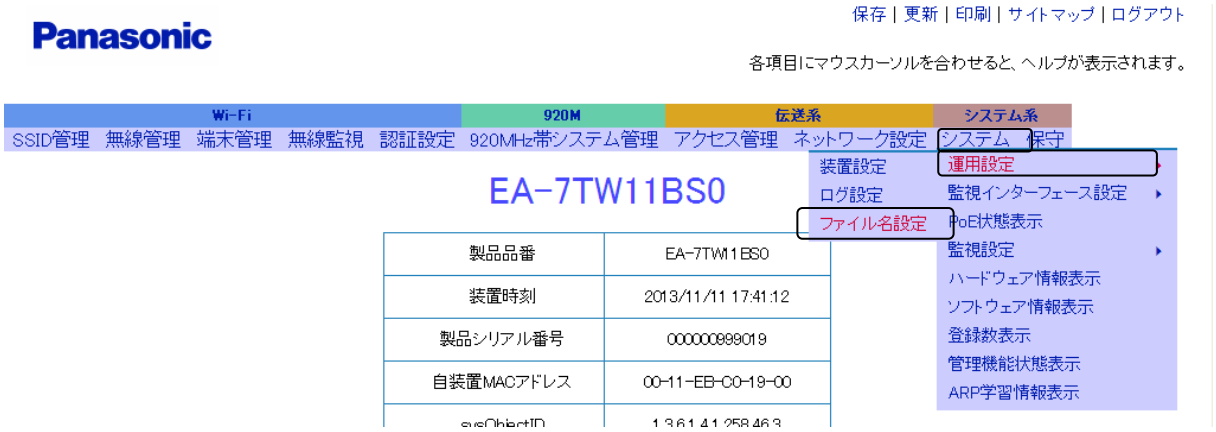


図7.1-1　メニュー（ファイル名設定）

手順2　設定ファイルのファイル名を入力します。（拡張子は不要）

例として、「config」を入力します。
ここで設定したファイル名が、バックアップファイル名となります。

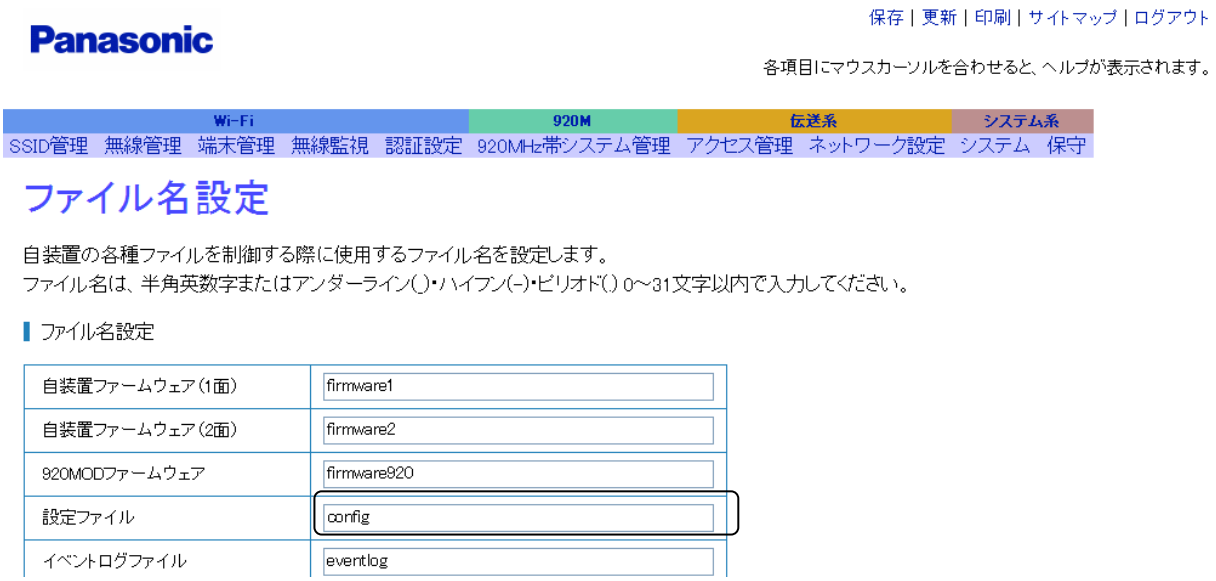


図7.1-2　ファイル名設定

手順3　画面最下部の〔設定〕をクリックし、設定を反映させます。

手順4　Windows の〔スタート〕をクリックし、〔すべてのプログラム〕
→　〔アクセサリ〕　→　〔コマンド プロンプト〕をクリックします。

手順5　〔コマンドプロンプト〕画面が表示されたら、バックアップした設定データを保存したいディレクトリへ移動します。

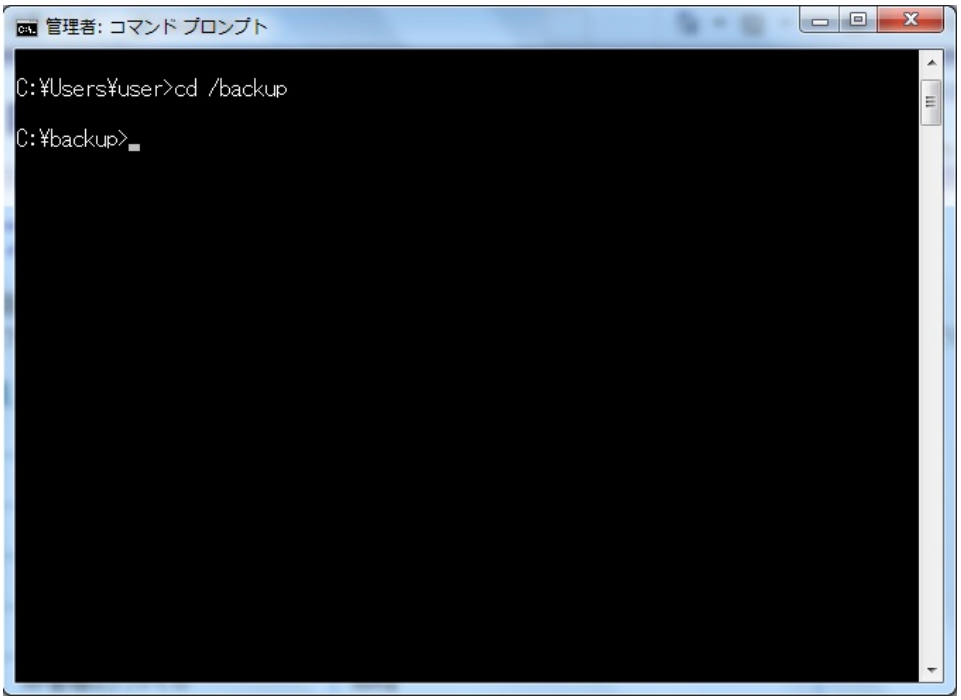


図7.1-3　設定ファイルバックアップ（コマンド）①

手順6　ftp コマンドを使って、WEB コンソール用 PC からコンセントレータに接続します。
コンセントレータの IP アドレスを「192.168.0.3」とした場合のコマンド入力例を示します。

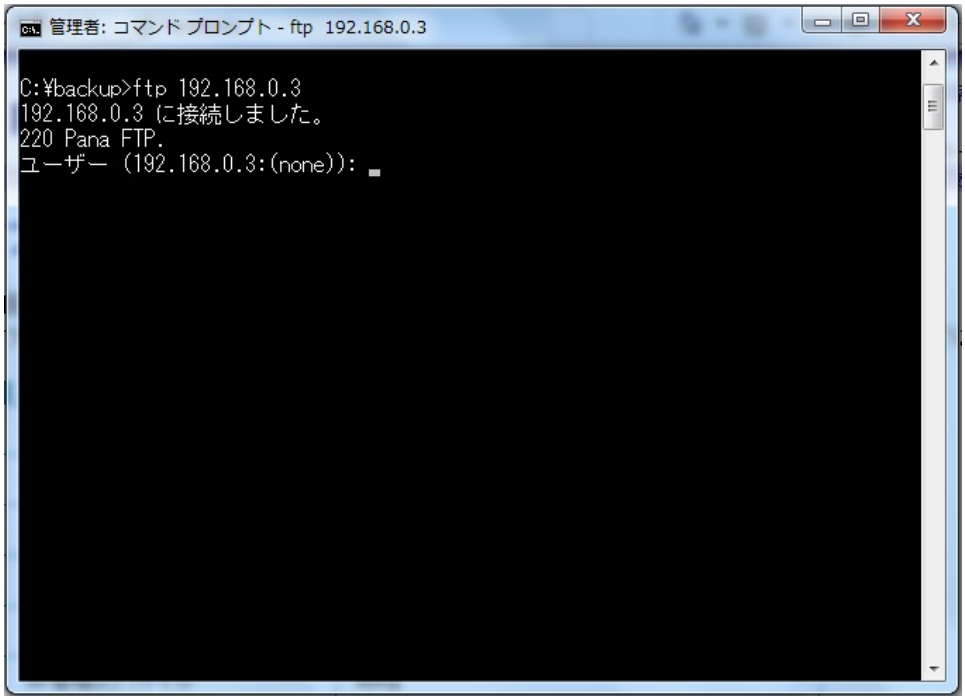


図7.1-4　設定ファイルバックアップ（コマンド）②

手順7　パスワードを入力し、実行します。

例として、管理者権限（ここでは初期値の「root」）を入力します。

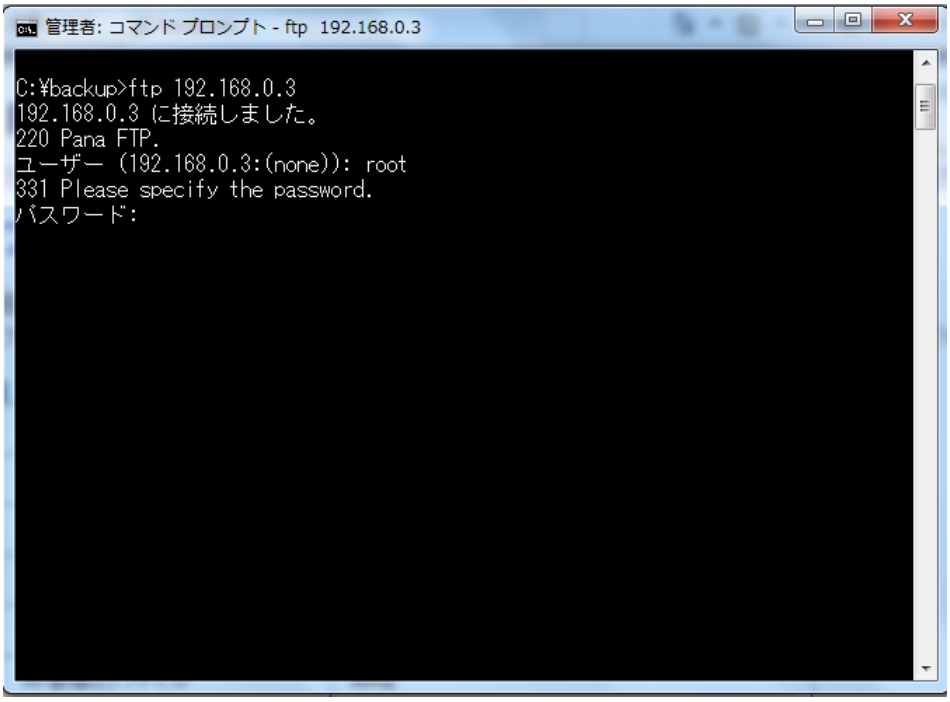


図7.1-5　設定ファイルバックアップ（コマンド）③

手順8　パスワードを入力し、実行します。

パスワード入力時、画面に入力内容は表示されません。

ログインが成功した場合は、「Login successful.」と表示されます。

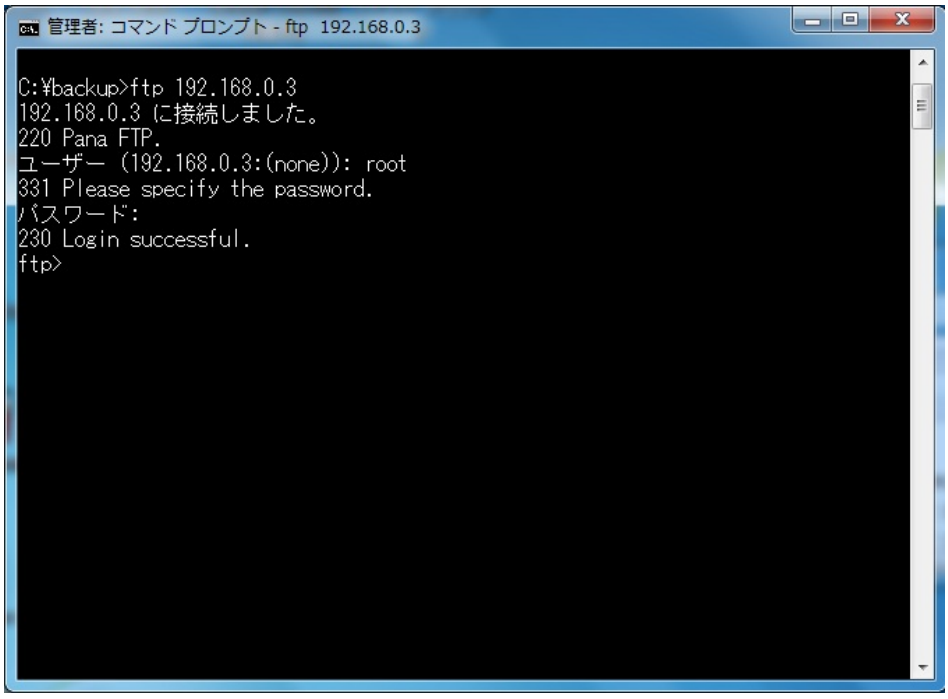


図7.1-6　設定ファイルバックアップ（コマンド）④

手順9　設定ファイルをバックアップします。

ここでは、設定ファイルのファイル名を「setting」として、下記コマンドを入力／実行します。

コマンド：“get setting”

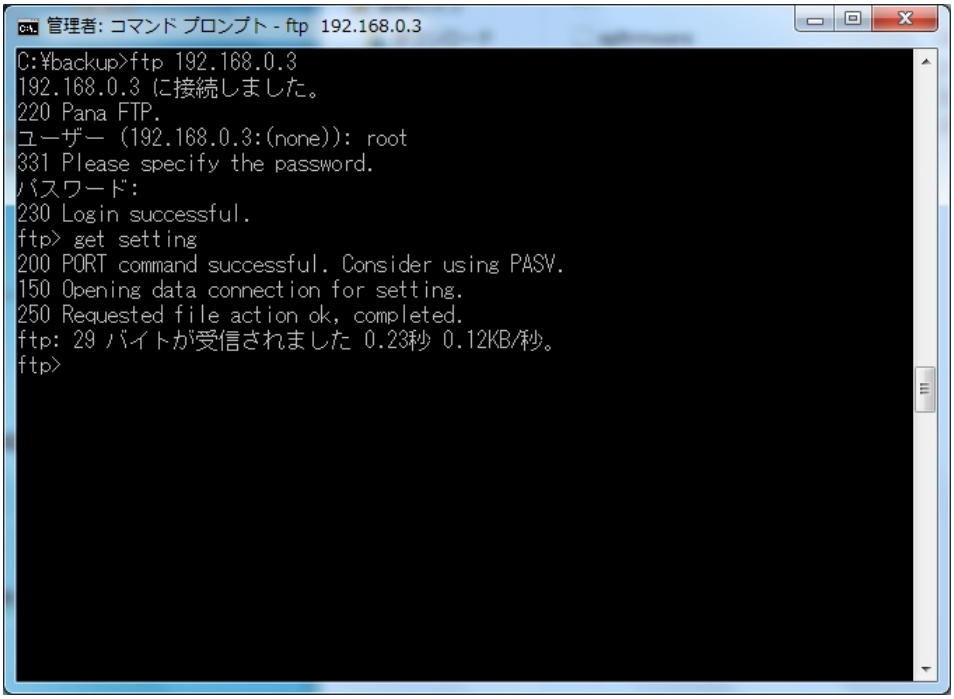


図7.1-7　設定ファイルバックアップ（コマンド）⑤

手順10　ログアウトし、ftp を終了します。

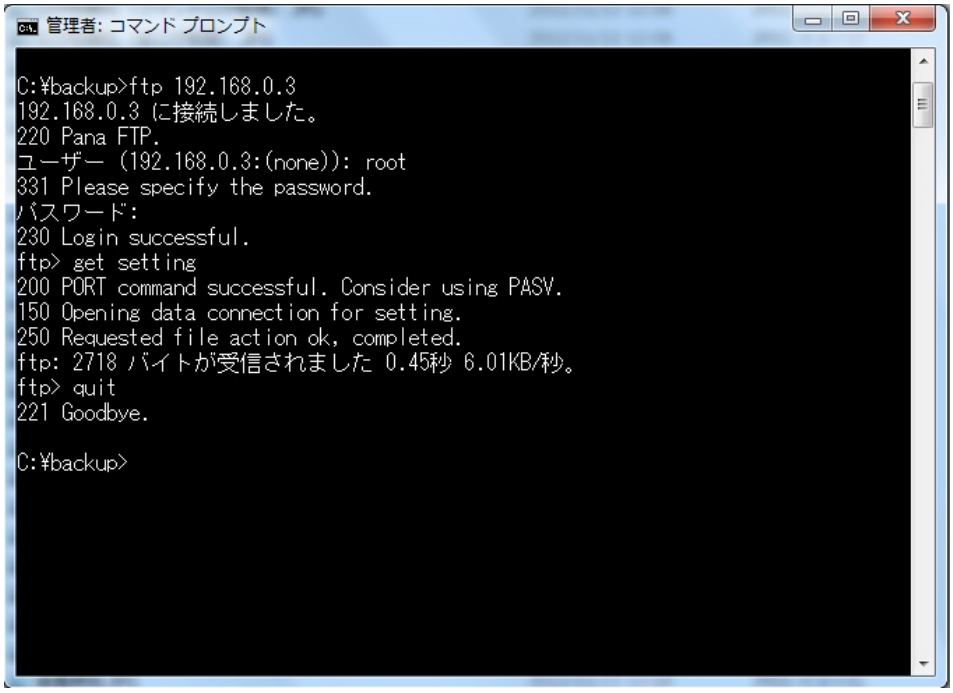


図7.1-8　設定ファイルバックアップ（コマンド）⑥

※Windows XP では、tftp コマンドでの設定ファイルバックアップも可能です。

7.1.2　設定データの読み込み

コンセントレータで設定データを読み込む方法は、コンセントレータに接続している PC より FTP コマンドを使用する方法、WEB コンソールでファイルコピーを使用する方法があります。ここでは、FTP コマンドを使用してコンセントレータに接続している PC よりコンセントレータへ設定ファイルを読み込む方法を紹介します。

操作手順

手順1　～　手順４は、「6.1.1　設定データのバックアップ」を参照してください。

手順5　保存している設定データのディレクトリへ移動します。

ここでは、「C:\backup」に「setting」という名称の設定ファイルを保存しているものとします。

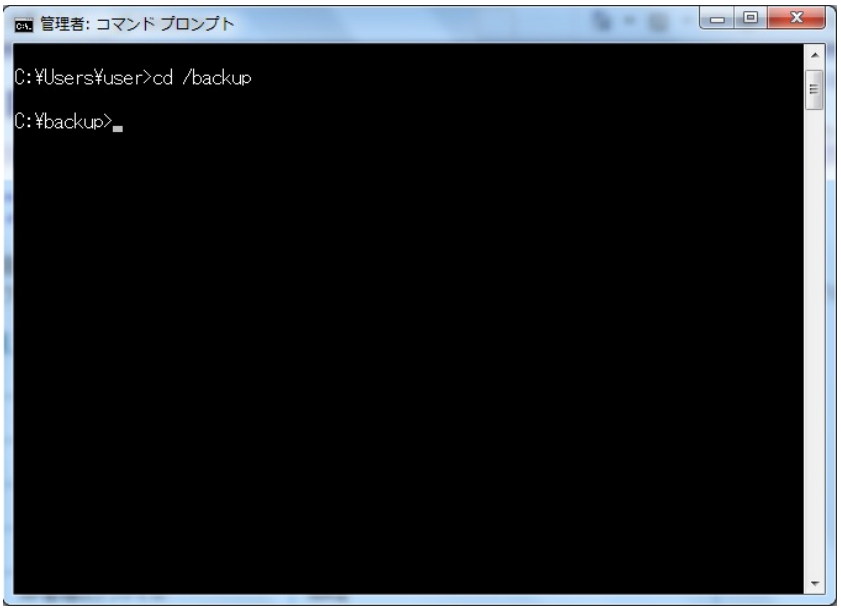


図7.1-9　設定ファイル読み込み（コマンド）①

手順6　ftp コマンドを使って、WEB コンソール用 PC からコンセントレータに接続します。

コンセントレータの IP アドレスを「192.168.0.3」とした場合のコマンド入力例を示します。

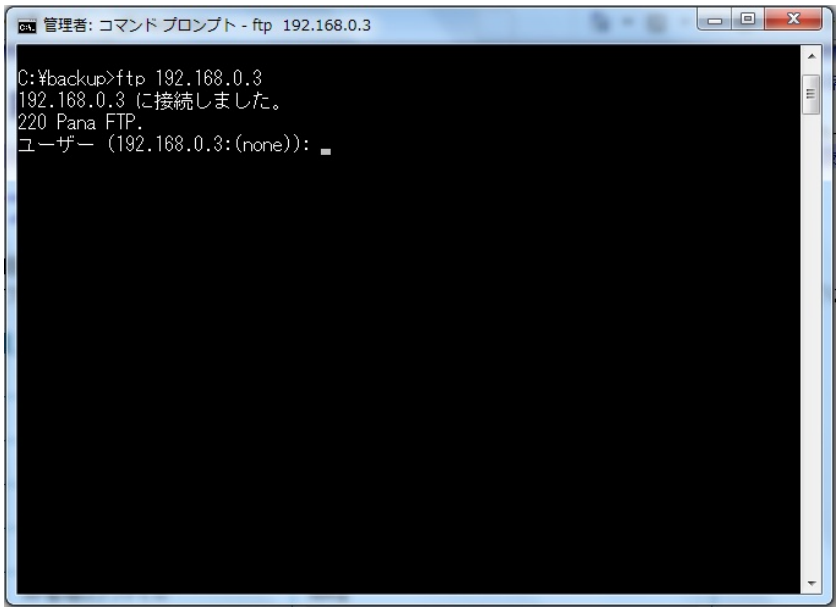


図7.1-10　設定ファイル読み込み（コマンド）②

手順7　ユーザ名を入力し、実行します。

例として、管理者権限（ここでは初期値の「root」）を入力します。

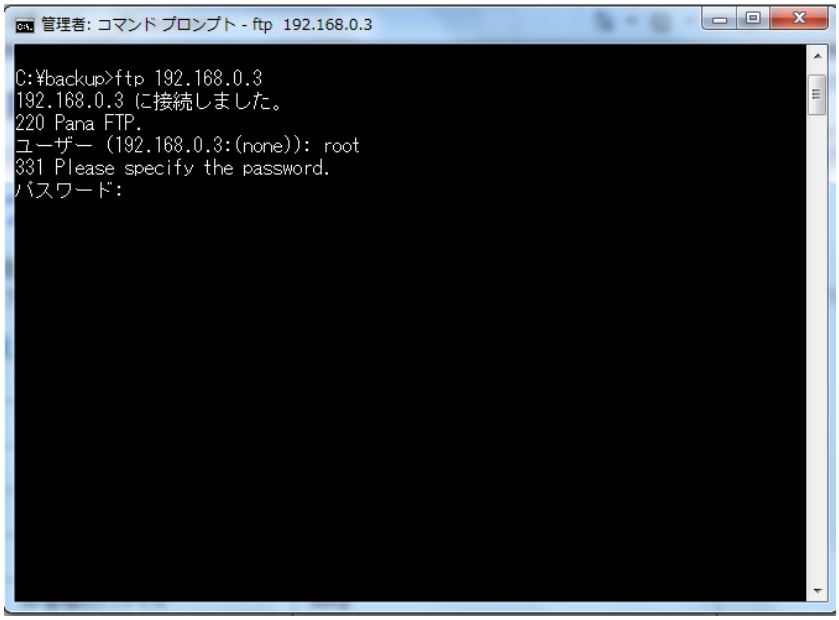


図7.1-11　設定ファイル読み込み（コマンド）③

手順8　パスワードを入力し、実行します。

パスワード入力時、画面に入力内容は表示されません。

ログインが成功した場合は、「Login successful」と表示されます。

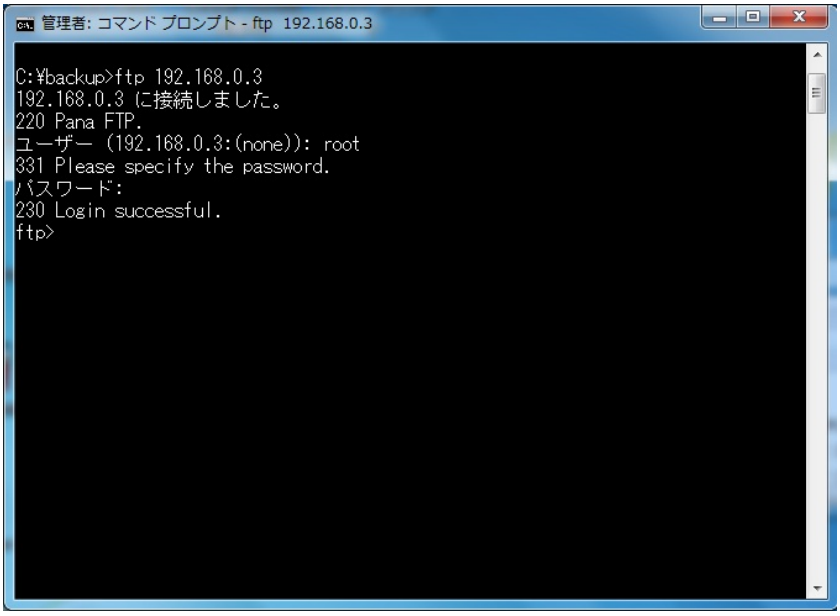


図7.1-12　設定ファイル読み込み（コマンド）④

手順9　設定ファイルを読み込みます。

ここでは、設定ファイルのファイル名を「setting」として、下記コマンドを入力／実行します。

コマンド：“put setting”

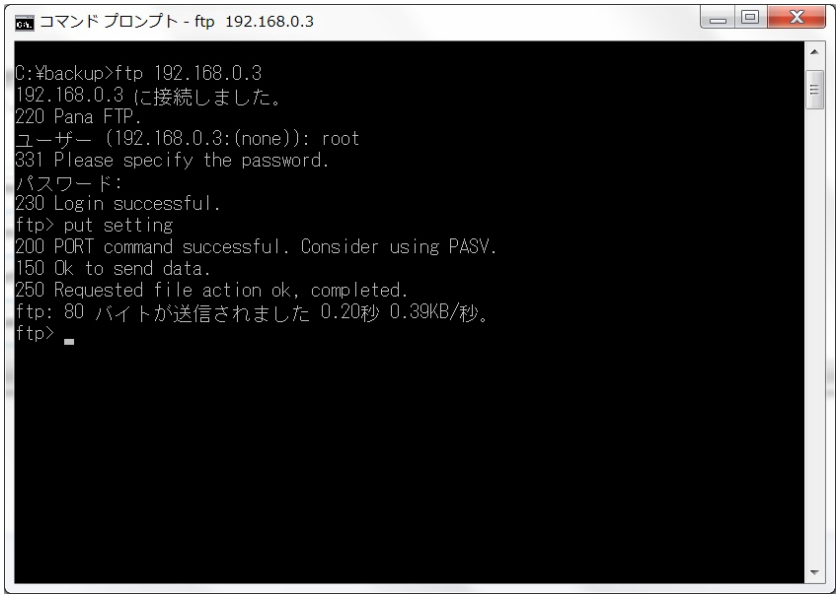


図7.1-13　設定ファイル読み込み（コマンド）⑤

手順10　ログアウトし、ftp を終了します。

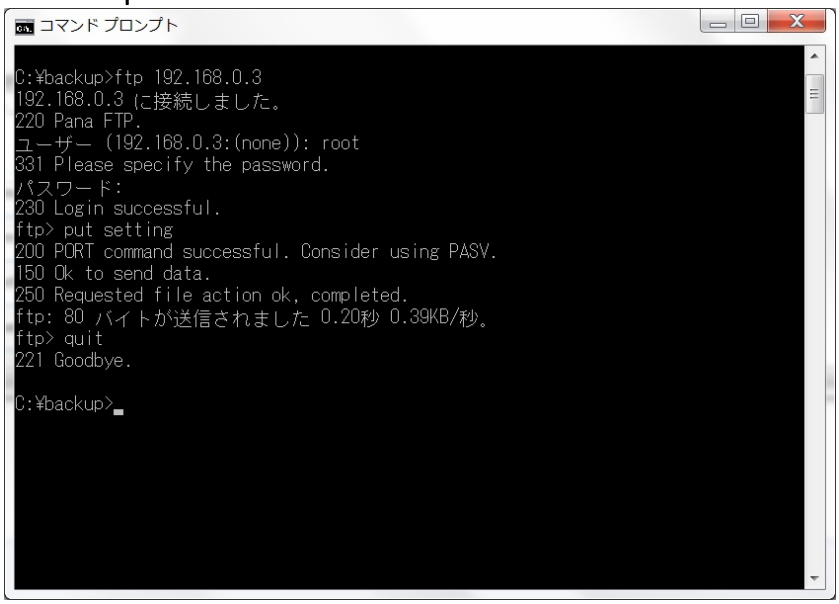


図7.1-14　設定ファイル読み込み（コマンド）⑥

※　　では、tftp コマンドでの設定ファイル読み込みも可能です。

7.1.3　全設定一括バックアップ

コンセントレータの全設定データを一括バックアップする方法は、FTP コマンドを使用する方法、WEB コンソールでファイルコピーを使用する方法、CLI コンソールでコマンドを実行する方法があります。ここでは、FTP コマンドを使用して、WEB コンソールに接続している PC に設定ファイルをバックアップする方法を紹介します。

操作手順

手順1　〔システム設定〕　→　〔運用設定〕　→　〔ファイル名設定〕を選択します。

図7.1-15　メニュー（ファイル名設定）

手順2　設定ファイルのファイル名を入力します。（拡張子は不要）

例として、「allconfig」を入力します。

ここで設定したファイル名が、バックアップファイル名となります。

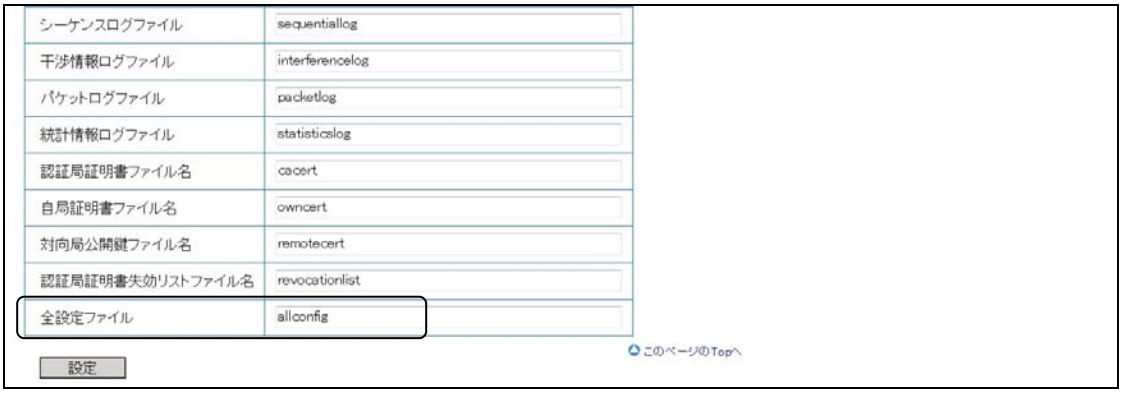


図7.1-16　ファイル名設定

手順3　画面最下部の〔設定〕をクリックし、設定を反映させます。

手順4　Windows の〔スタート〕をクリックし、〔すべてのプログラム〕
→　〔アクセサリ〕　→　〔コマンド プロンプト〕をクリックします。

手順5　〔コマンドプロンプト〕画面が表示されたら、バックアップした設定データを保存したいディレクトリへ移動します。

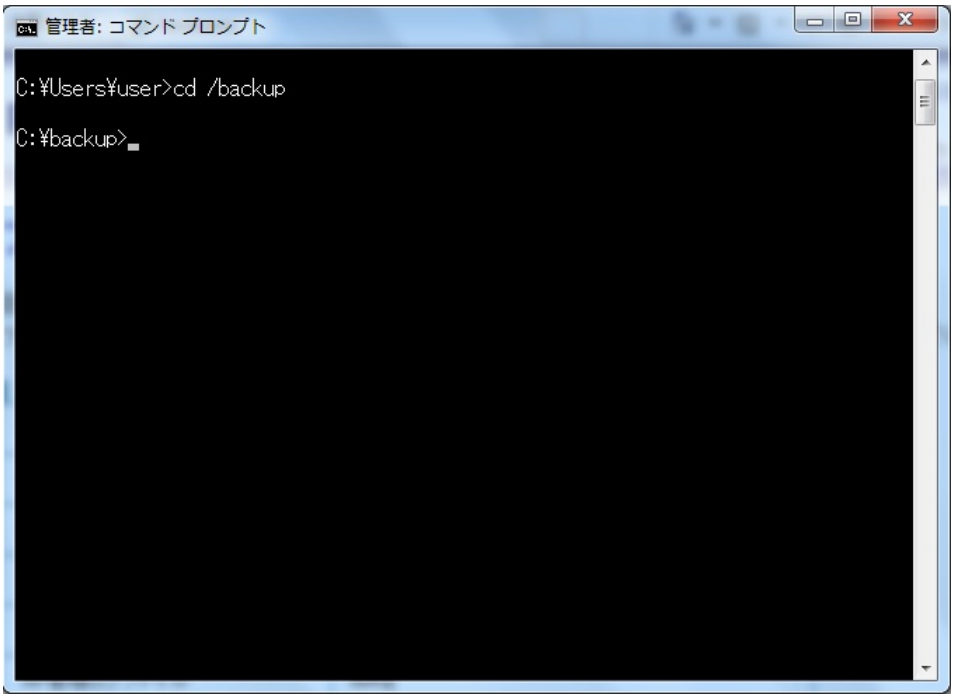


図7.1-17　全設定一括バックアップ（コマンド）①

手順6　ftp コマンドを使って、WEB コンソール用 PC からコンセントレータに接続します。

コンセントレータの IP アドレスを「192.168.0.3」とした場合のコマンド入力例を示します。

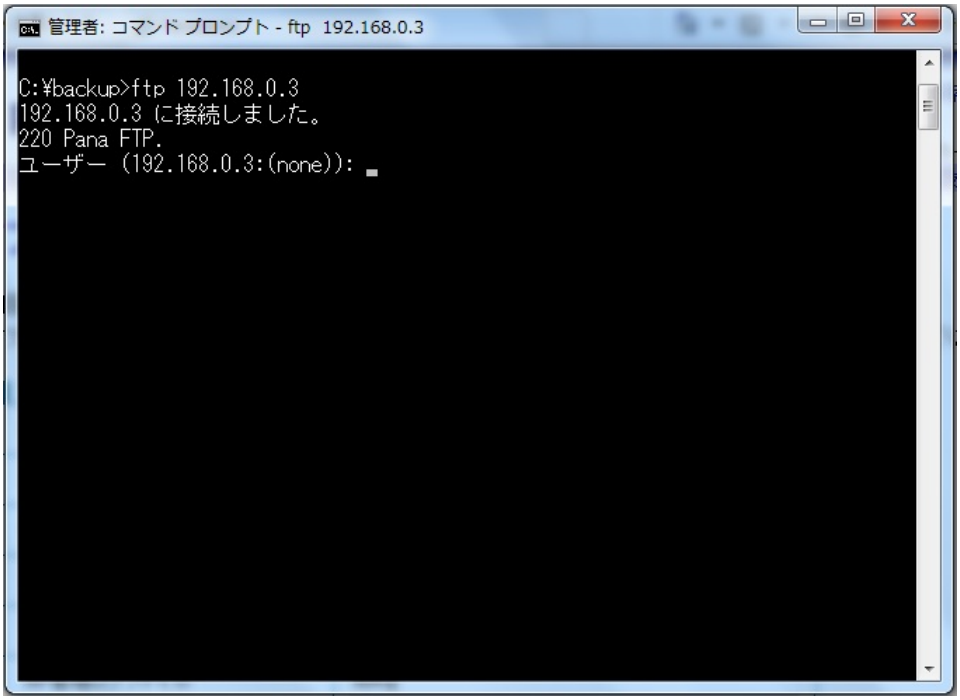


図7.1-18　全設定一括バックアップ（コマンド）②

手順7　ユーザ名を入力し、実行します。

例として、管理者権限（ここでは初期値の「root」）を入力します。

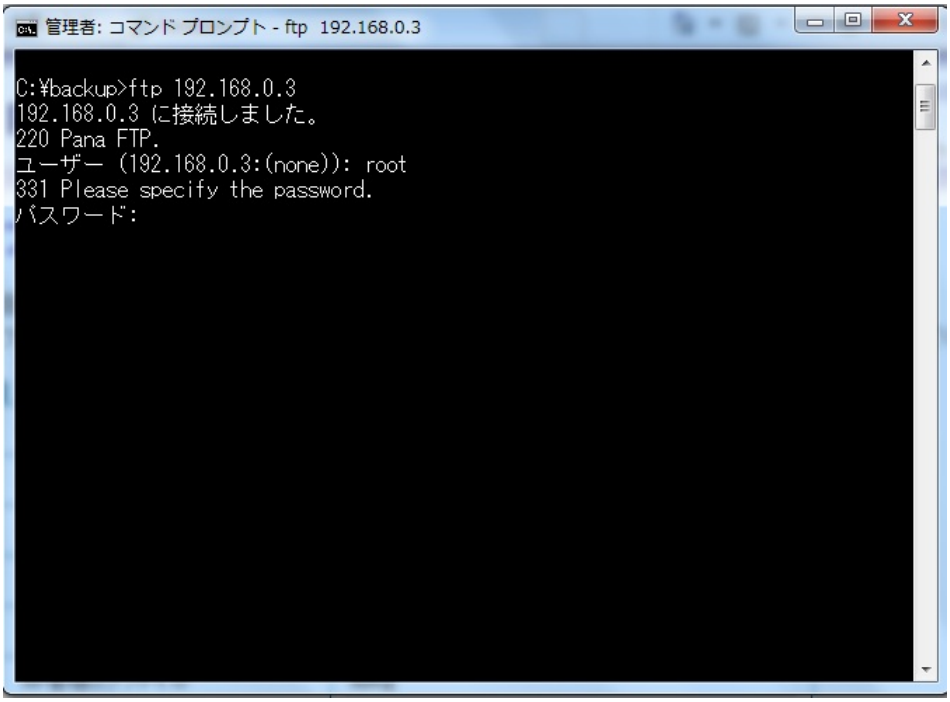


図7.1-19　全設定一括バックアップ（コマンド）③

手順8　パスワードを入力し、実行します。

パスワード入力時、画面に入力内容は表示されません。

ログインが成功した場合は、「Login successful.」と表示されます。

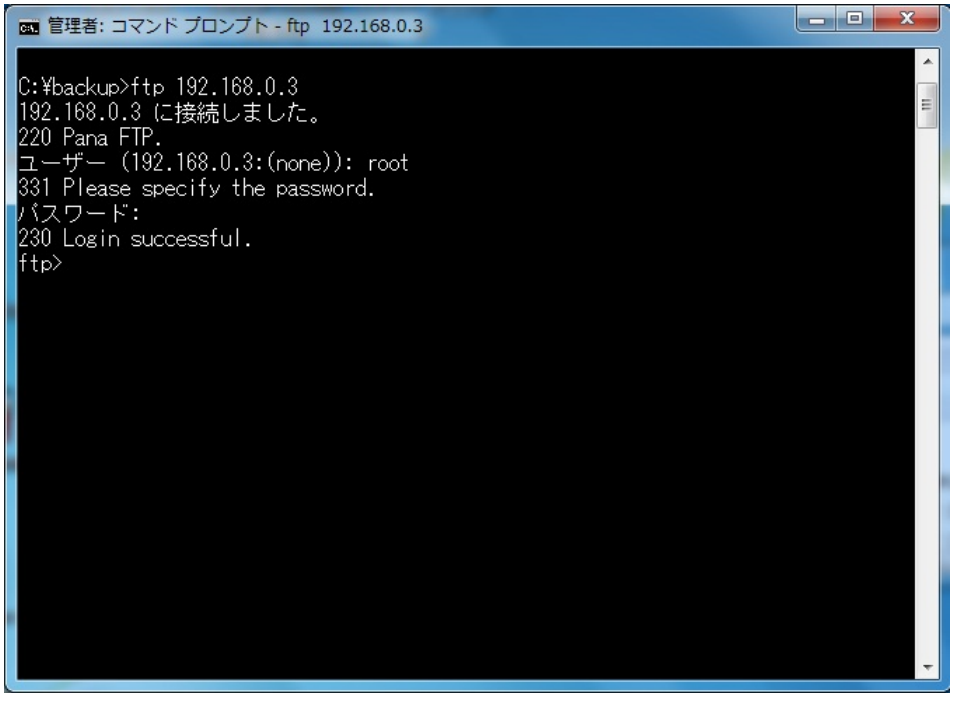


図7.1-20　全設定一括バックアップ（コマンド）④

手順9　設定ファイルをバックアップします。

ここでは、設定ファイルのファイル名を「allconfig」として、下記コマンドを入力／実行します。

コマンド：“binary”

コマンド：“get allconfig”

図7.1-21　全設定一括バックアップ（コマンド）⑤

手順10　ログアウトし、ftp を終了します。

図7.1-22　全設定一括バックアップ（コマンド）⑥

※Windows XP では、tftp コマンドでの全設定一括バックアップも可能です。

7.1.4　全設定一括読み込み

コンセントレータで全設定を一括で読み込む方法は、コンセントレータに接続している PC より FTP コマンドを使用する方法、WEB コンソールでファイルコピーを使用する方法があります。ここでは、FTP コマンドを使用してコンセントレータに接続している PC よりコンセントレータへ設定ファイルを読み込む方法を紹介します。

操作手順

手順1　～　手順４は、「6.1.3　全設定一括バックアップ」を参照してください。

手順5　保存している設定データのディレクトリへ移動します。

ここでは、「C:\backup」に「allconfig」という名称の設定ファイルを保存しているものとします。

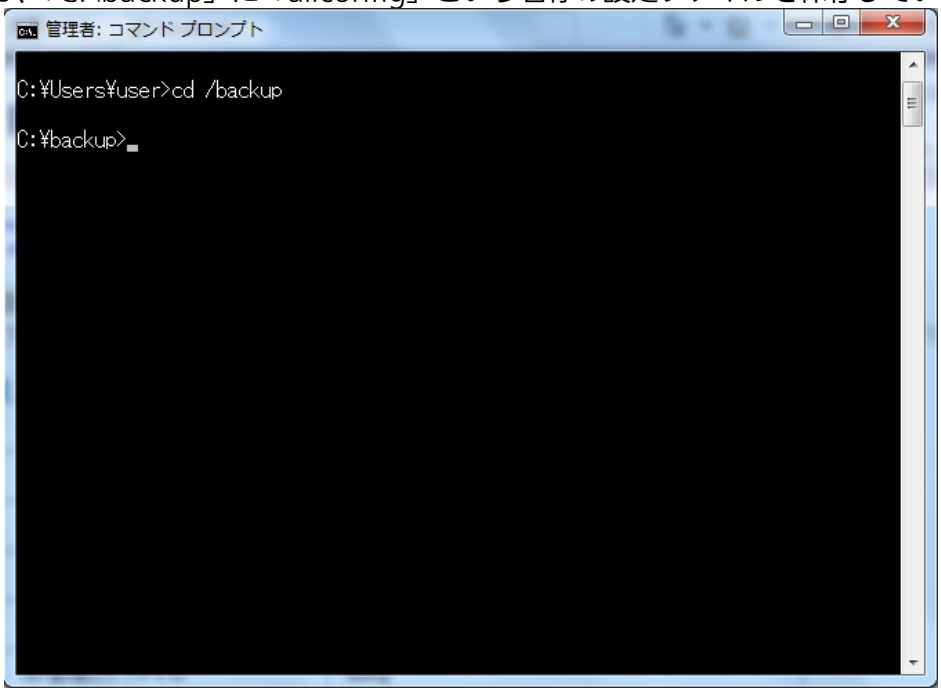


図7.1-23　全設定一括読み込み（コマンド）①

手順6　ftp コマンドを使って、WEB コンソール用 PC からコンセントレータに接続します。

コンセントレータの IP アドレスを「192.168.0.3」とした場合のコマンド入力例を示します。

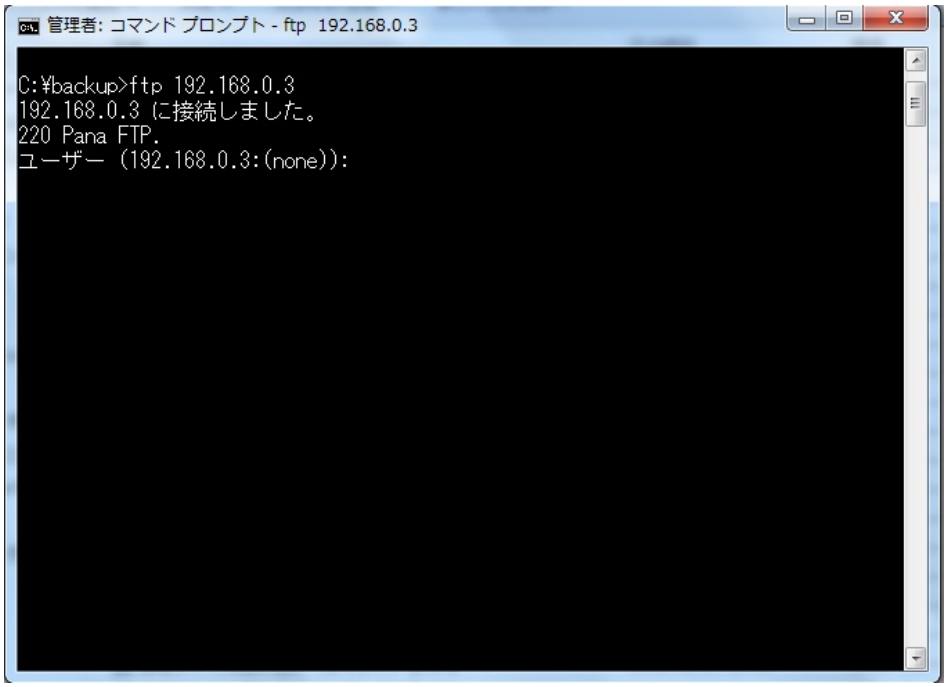


図7.1-24　全設定一括読み込み（コマンド）②

手順7　ユーザ名を入力し、実行します。

例として、管理者権限（ここでは初期値の「root」）を入力します。

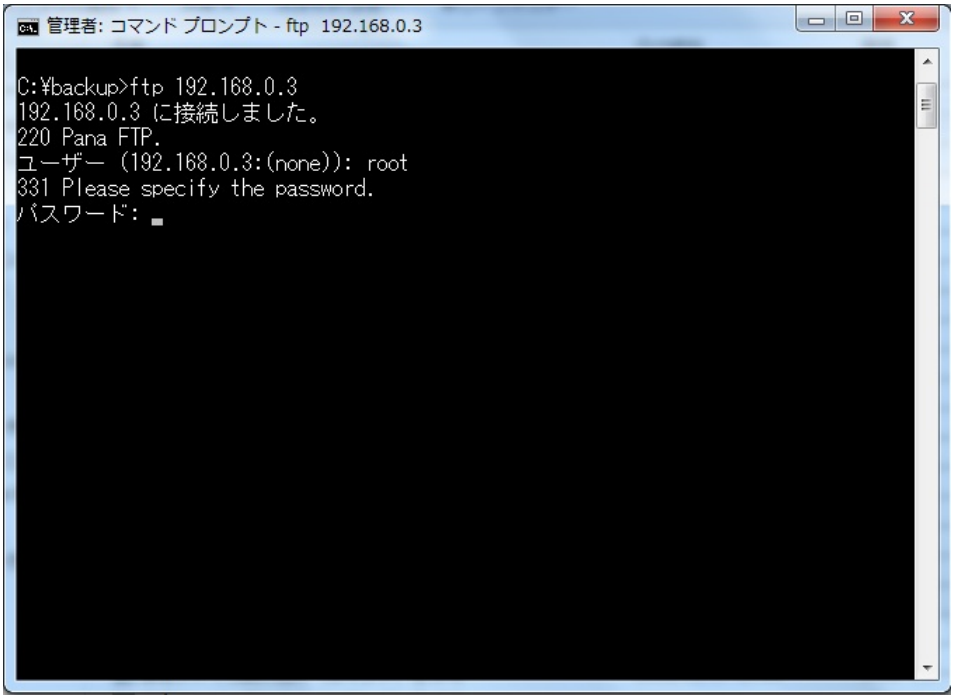


図7.1-25　全設定一括読み込み（コマンド）③

手順8　パスワードを入力し、実行します。

パスワード入力時、画面に入力内容は表示されません。

ログインが成功した場合は、「Login successful.」と表示されます。

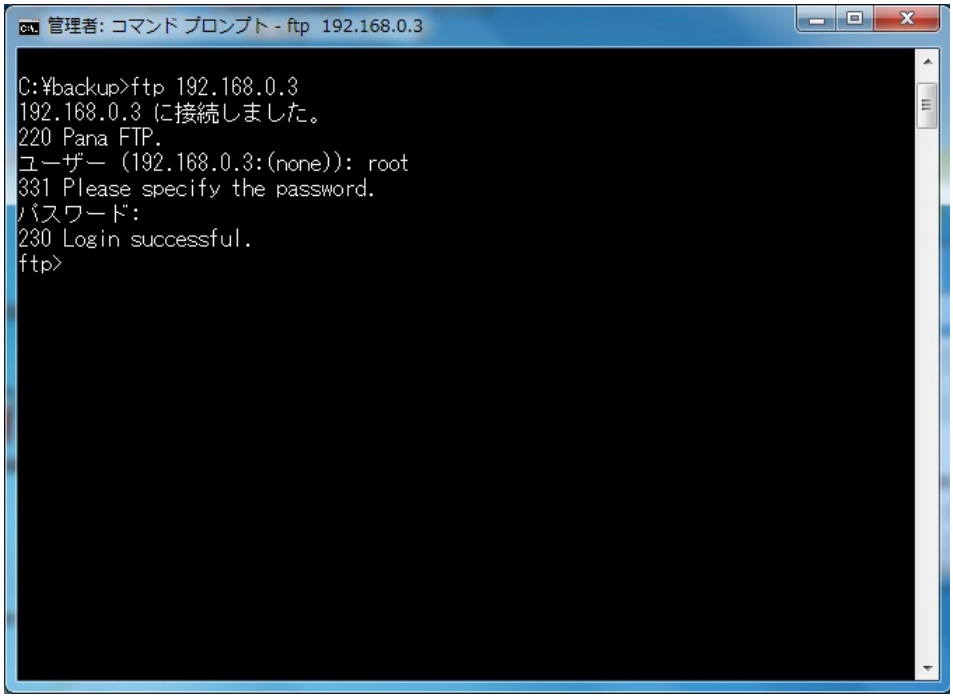


図7.1-26　全設定一括読み込み（コマンド）④

手順9　設定ファイルを読み込みます。

ここでは、設定ファイルのファイル名を「allconfig」として、下記コマンドを入力／実行します。

コマンド：　“binary”

コマンド：　“put allconfig”

図7.1-27　全設定一括読み込み（コマンド）⑤

手順10　ログアウトし、ftp を終了します。

図7.1-28　全設定一括読み込み（コマンド）⑥

※Windows XP では、tftp コマンドでの全設定一括読み込みも可能です。

重要	全設定一括読み込みが完了した後、Web 画面もしくは CLI コンソール上から設定の保存を実行せずに、そのまま装置をリセットしてください。リセット前に設定の保存を実行すると、読み込んだ全設定が、現在起動中の設定で上書きされてしまいますのでご注意ください。

7.2　ファームウェアのアップデート

コンセントレータでは、手動にてファームウェアをアップデートすることができます。ファームウェアをアップデートする方法の１つとして、FTP を利用する方法を紹介します。
ここでは、入手したファームウェアが、コンソールとしてコンセントレータに接続している PC に保存されているという前提で、コンセントレータのファームウェアのアップデートを行います。

操作手順

手順1　〔システム系〕 → 〔システム〕 → 〔運用設定〕 → 〔ファイル名設定〕を選択します。

図7.2-1　メニュー（ファイル名設定）

手順2　読み込むファームウェアのファイル名を指定します。（拡張子は不要）
例として、自装置ファームウェア（1 面）に「firmware1」を入力します。

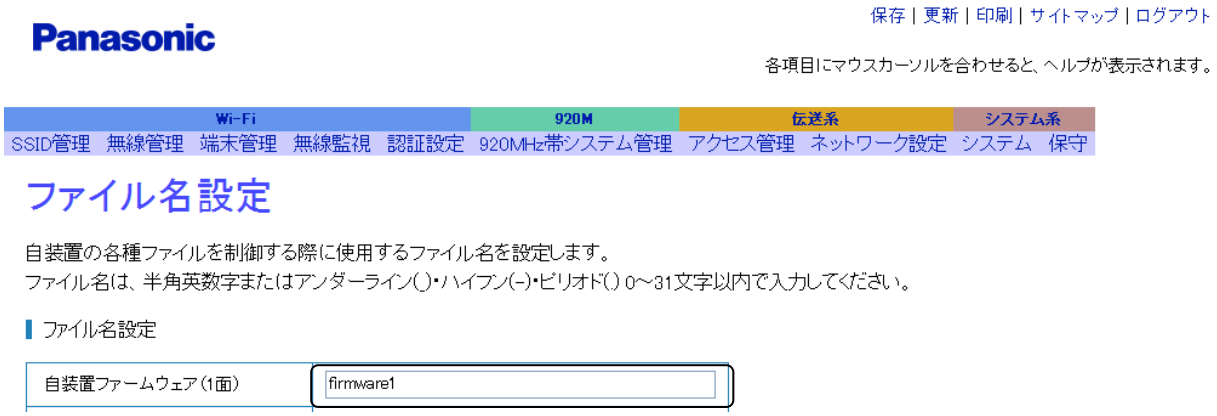


図7.2-2　ファイル名設定

手順3　画面最下部の〔設定〕をクリックし、設定を反映させます。
手順4　Windows の〔スタート〕をクリックし、〔すべてのプログラム〕
→ 〔アクセサリ〕 → 〔コマンド プロンプト〕をクリックします。

手順5　〔コマンドプロンプト〕画面が表示されたら、ファームウェアが保存されているディレクトリへ移動します。

ここでは、「C:\backup」に「firmware1」という名称の設定ファイルを保存しているものとします。

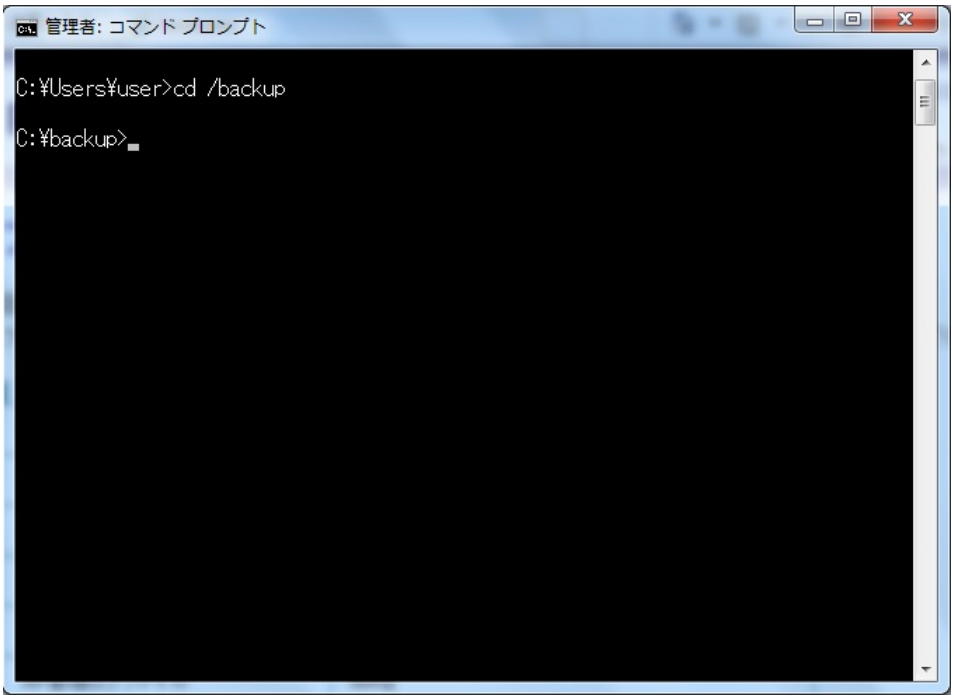


図7.2-3　ファームウェアのアップデート①

手順6　ftp コマンドを使って、WEB コンソール用 PC からコンセントレータに接続します。

コンセントレータの IP アドレスを「192.168.0.3」とした場合のコマンド入力例を示します。

図7.2-4　ファームウェアのアップデート（コマンド）②

手順7　ユーザ名を入力し、実行します。

例として、管理者権限（ここでは初期値の「root」）を入力します。

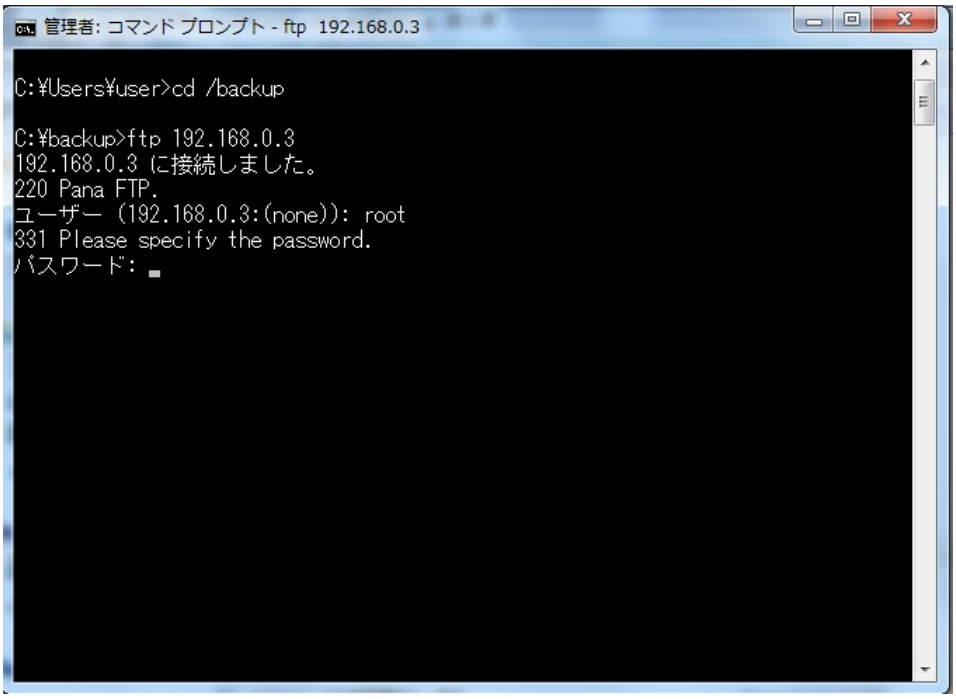


図7.2-5　ファームウェアのアップデート（コマンド）③

手順8　パスワードを入力し、実行します。

パスワード入力時、画面に入力内容は表示されません。

ログインが成功した場合は、「Login successful.」と表示されます。

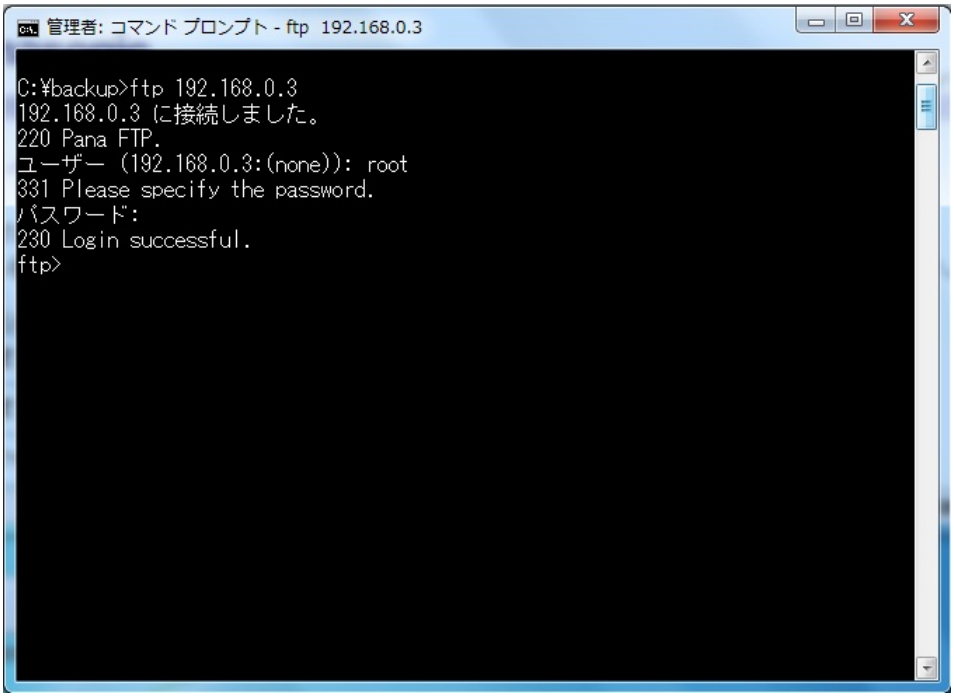


図7.2-6　ファームウェアのアップデート（コマンド）④

手順9　ftp コマンドを使って、コンセントレータに接続中の PC よりファームウェアを読み込みます。
コンセントレータの IP アドレスを「192.168.0.3」、アップデート用ファームウェアのファイル名を「apfirmware」とした場合のコマンド入力例を示します。

コマンド：“put apfirmware”

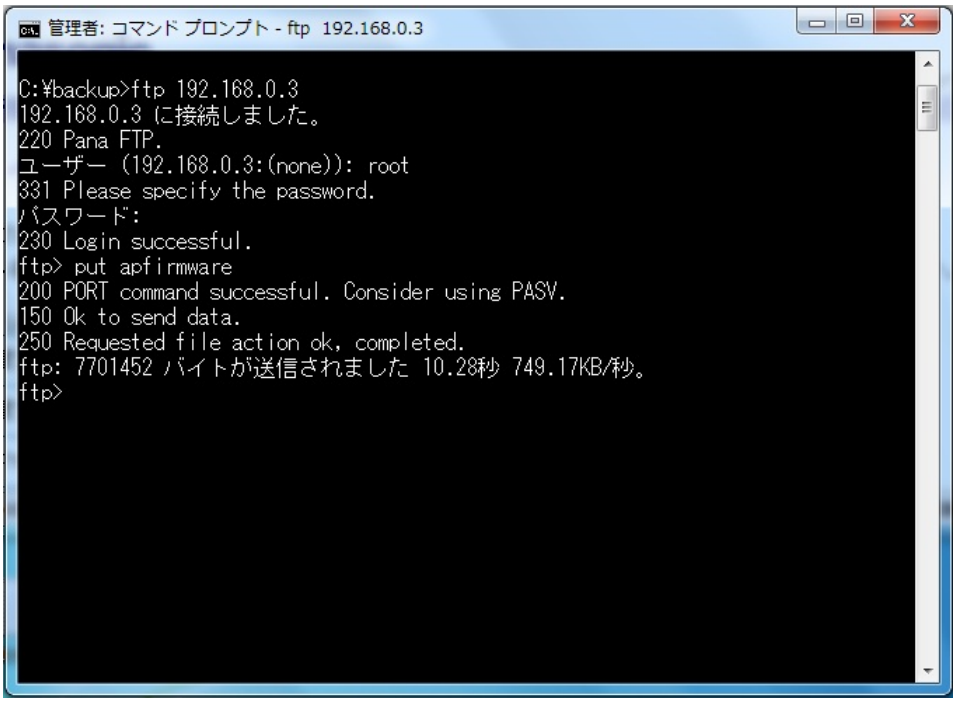


図7.2-7　ファームウェアのアップデート⑤

手順 9 を実行後、ファームウェアのアップデート処理開始となります。

手順10　コンセントレータをリセットし、読み込んだファームウェアを有効にします。
ftp の転送が完了した時点でファームウェアの更新は完了しています。コンセントレータ のリセットを行ってください。

以上の操作により、ファームウェアのアップデートが完了となります。以下では、アップデートしたファームウェアのバージョン確認方法を紹介します。

手順11　〔システム系〕　→　〔システム〕　→　〔ソフトウェア情報表示〕を選択します。

図7.2-8　メニュー（ソフトウェア情報表示）

手順12　アップデートしたファームウェアのバージョンを確認します。

図7.2-9　ソフトウェア情報表示

上記、手順 11 と手順 12 により、ファームウェアのバージョンを確認することができます。

7.3　ログ機能

コンセントレータでは、システムを運用管理するために有効なトラフィック統計情報や各種イベントなどをログデータとして蓄積し、コンソール上から表示、確認することができます。また、コンセントレータ内に蓄積されたログデータは、FTP（TFTP）サーバに書き出すことが可能です。

※CLI コンソールでは、蓄積したログデータの読み出しには show コマンドを使用します。show コマンドについて詳しくは、コマンドリファンレスを参照してください。

7.3.1　ログ一覧

コンセントレータが持つログデータの一覧を以下に示します。

表7.3-1　ログデーター一覧

モード名称	説明	データ保持	最大蓄積数
イベントログ	・セルフテスト結果 ・各種障害状態 ・AP 接続状態	電源 OFF 時ログデータ保持	512
AP 管理ログ	・AP 制御 ・AP 状態	電源 OFF 時ログデータ保持	512
端末管理ログ	・端末制御 ・端末状態 ・QoS 制御	保持なし	50,000
TRAP ログ	・Trap 送信	保持なし	256
アクセスログ	・Telnet アクセス ・TFTP アクセス ・FTP アクセス ・SNMP アクセス ・NTP アクセス ・HTTP アクセス　　等	保持なし	512
設定ログ	・設定関係	保持なし	256
シーケンスログ	・Authentication ・Association ・Reassociation ・無線制御	保持なし	3072
干渉情報ログ	・周辺 AP の RSSI 値 ・ノイズフロア値	保持なし	786,432 （6Mbytes 分）
パケットログ	・管理フレーム ・認証フレーム	保持なし	500,000 （128Mbytes 分）
統計情報ログ	・端末接続台数 ・端末接続拒否回数	保持なし	180,000 （ 約　16Mbytes 分）

※　「電源 OFF 時ログデータ保持」となっているログは、10 分ごと、またはリセット実施時に揮発領域から不揮発性領域に書き込み保存します。電源断をした場合は、不揮発性領域に保存後の 10 分間のデータ（不揮発性領域に保存される前の揮発性領域のデータ）は補償されません。

※　WEB コンソール・CLI コンソール・コマンドプロンプトでの FTP（TFTP）を使用して、ログ読出しが可能です。ただし、干渉情報ログ・パケットログ・統計情報ログの 3 つのログは、情報量が膨大なため、WEB コンソール・CLI コンソールでのログ読出しができません。

※ 干渉情報ログ・パケットログ・統計情報ログはバイナリデータであり、バイナリ転送モードで読み出す必要があります。
※ TFTP は UDP 接続で信頼性に欠けるため、大容量ファイルを転送する場合は FTP をご使用ください。

7.3.2　記録・表示

コンセントレータのログを記録・表示するための手順をここで紹介します。

操作手順

◆ログ機能の有効化

ログ機能を有効にするために、監視制御設定を行います。

手順1　〔システム系〕　→　〔保守〕　→　〔監視制御設定〕を選択します。

図7.3-1　メニュー（監視制御設定）

手順2　監視制御の〔ON〕を選択し、〔設定〕をクリックします。

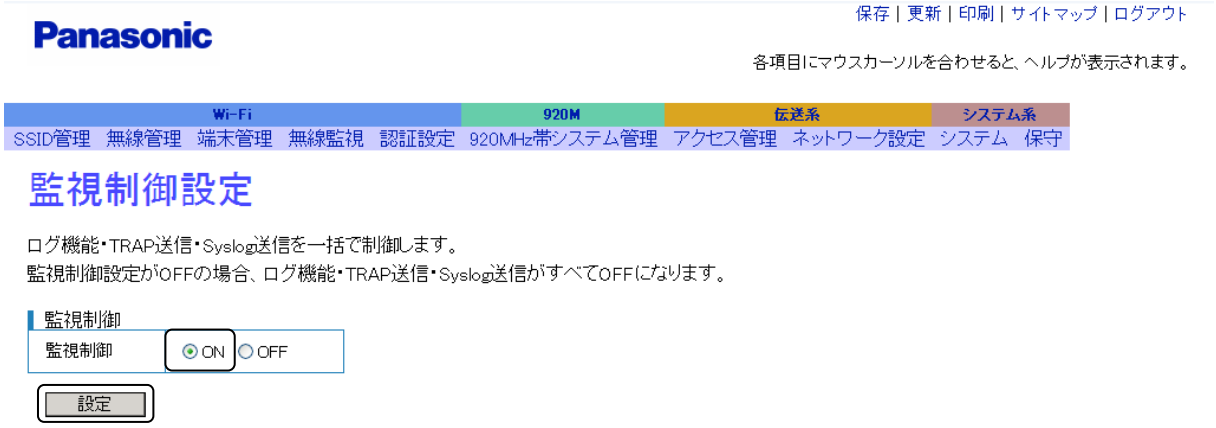


図7.3-2　監視制御設定

※　このオプションは、ログ機能だけでなく、ログ機能・TRAP 送信・Syslog 送信などすべての監視制御機能の ON/OFF を一括で切り替えます。

手順3　画面右上の〔保存〕をクリックし、設定した内容をコンセントレータに保存します。

◆ログのファイル名設定

各種ログファイルのファイル名を設定します。

手順4　〔システム系〕　→　〔システム〕　→　〔運用設定〕　→　〔ファイル名設定〕を選択します。

図7.3-3　メニュー（ファイル名設定）

手順5　各種ログのファイル名を入力します。

図7.3-4　ファイル名設定

手順6　画面最下部の〔設定〕をクリックし、設定を反映させます。

◆ログの記録方法の設定

ログの取得方法など、ログの記録に関する詳細設定を行います。

手順7　〔システム系〕　→　〔システム〕　→　〔運用設定〕　→　〔ログ設定〕を選択します。

図7.3-5　メニュー（ログ設定）

※　手順 8 ～ 手順 10 は〔ログ設定〕画面（図 6.3-6）より各種設定を行います。

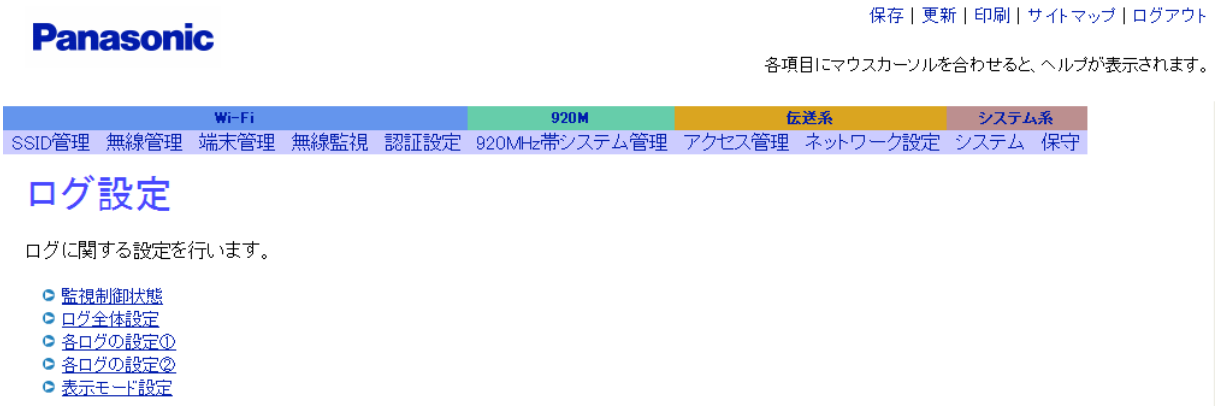


図7.3-6　ログ設定

手順8　〔ログ設定〕画面（図 6.3-6）の〔ログ全体設定〕をクリックし、〔有効〕を選択します。

図7.3-7　ログ全体設定

手順9　〔ログ設定〕画面（図 6.3-6）の〔各ログの設定①〕をクリックし、各ログの取得モードを選択します。

例として、すべて〔wrap〕を選択します。

図7.3-8　各ログの設定①

表7.3-2　ログ取得モード

モード名称	説明
wrap	ログが最大件数に達した場合に、最古のレコードから上書き保存します。
halt	ログが最大件数に達した場合は、それ以上ログ取得を行いません。 ログ消去でログ取得を再開します。
off	ログ取得は行いません。

手順10　〔ログ設定〕画面（図 6.3-6）の〔各ログの設定②〕をクリックし、ログの取得設定を行います。
例として、パケットログ・統計情報ログの取得を〔有効〕にします。

図7.3-9　各ログの設定②

手順11　画面最下部の〔設定〕をクリックし、設定を反映させた後、画面右上の〔保存〕をクリックし、設定した内容をコンセントレータに保存します。

以上の操作／設定により、ログを記録することができます。

◆ログデータの表示

「◆ログ機能の有効化」、「◆ログの記録方法の設定」を行って記録したログは、Web コンソール上で簡単に表示、確認できます。

ここでは、例としてコマンドログを表示する方法を紹介します。

手順12 〔システム系〕 → 〔保守〕 → 〔ログ表示〕 → 〔コマンドログ〕を選択します。

図7.3-10　メニュー（ログ表示）

以下の画面は、コマンドログの表示例です。

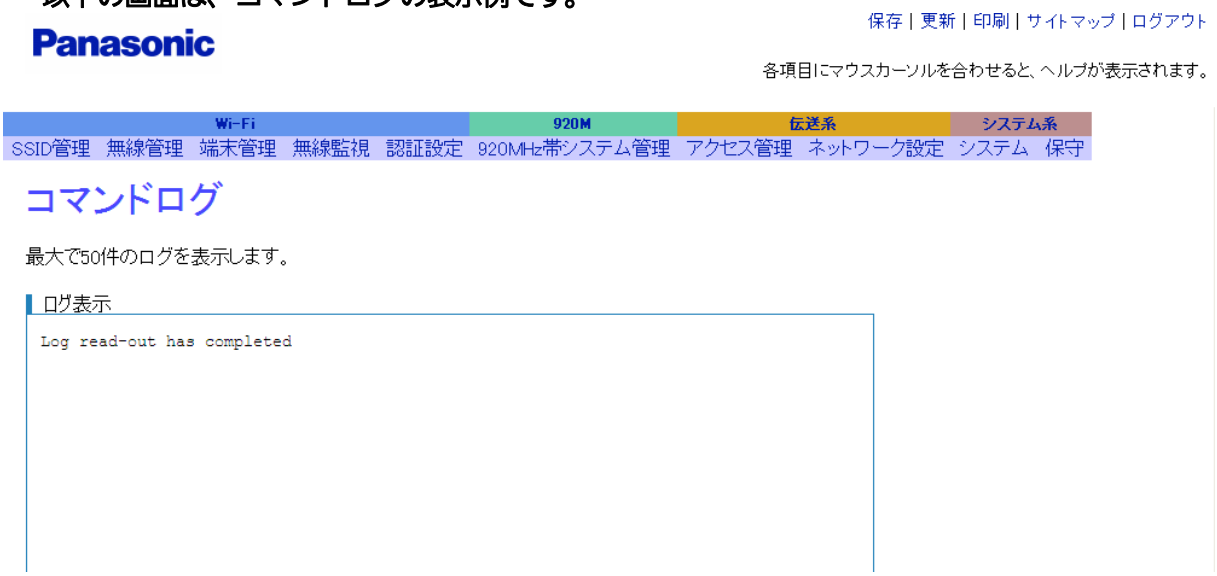


図7.3-11　コマンドログ

◆その他ログの読出し

コンセントレータでは、WEB 画面でのログ表示以外に、下記表（表 6.3-3　ログ読出し方法）に記載している方法での

ログ取得も行えます。

表7.3-3　ログ読出し方法

	説明
コマンドライン	通信ソフトを使用して、コマンド入力によりレコード単位に読み出しを行います。（別紙「コマンドリファレンス」参照）
TFTP	TFTP プロトコルにより一括読み出しを行います。（「6.3.3　FTP/TFTP によるリモート採取」参照）
syslog	syslog プロトコルにより syslog サーバへリアルタイムにログを転送します。（イベントログ、AP 管理ログ、端末管理ログのみ）

7.3.3　TFTP によるリモート採取

操作手順

◆TFTP サーバへのログファイルコピー

ログの記録は、前項ですでに済んでいるという前提で解説をします。

手順1　〔システム系〕　→〔システム〕　→　〔監視設定〕　→　〔TFTP 設定〕をクリックします。

図7.3-12　メニュー（TFTP 設定）

手順2　TFTP サーバとの通信に関する設定を入力します。

例として、下記内容での設定を示します。

- IP インターフェース番号に〔1〕を選択
- サーバ指定方法に〔IP アドレス〕を選択
- IP アドレス／ドメイン名に「192.168.0.241」（TFTP サーバのアドレス）を入力

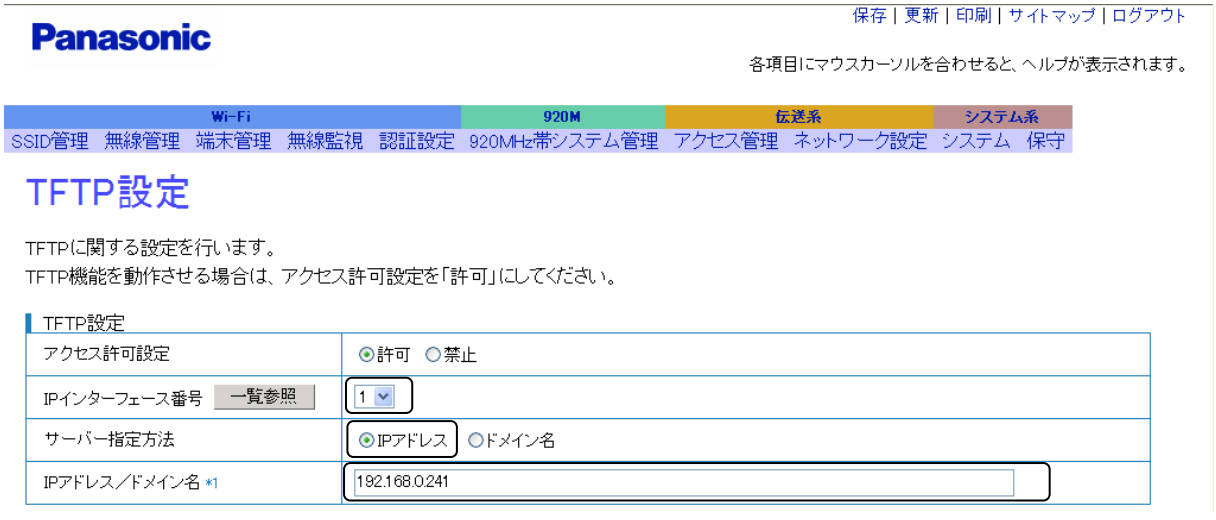


図7.3-13　TFTP 設定

手順3　TFTP 設定下部の〔設定〕をクリックし、設定を反映させます。

手順4　〔システム系〕　→　〔システム〕　→　〔運用設定〕　→　〔ファイル名設定〕を選択します。

図7.3-14　メニュー（ファイル名設定）

手順5　取得するログのファイル名を設定します。

例として、コマンドログを「command01」と設定します。

図7.3-15　ファイル名設定

手順6　画面最下部の〔設定〕をクリックし、設定を反映させた後、画面右上の〔保存〕をクリックし、設定した内容をコンセントレータに保存します。

手順7　〔保守〕　→　〔ファイルコピー〕を選択する。

図7.3-16　メニュー（ファイルコピー）

手順8　ファイルコピー方法とコピーするファイルを指定します。

例として、下記内容での設定を示します。

・ デバイス選択（コピー元→コピー先）で〔自装置→TFTP サーバ〕を選択

・ コピーファイルに「command01」を入力

選択、および入力後、画面左下の〔コピー〕をクリックします。

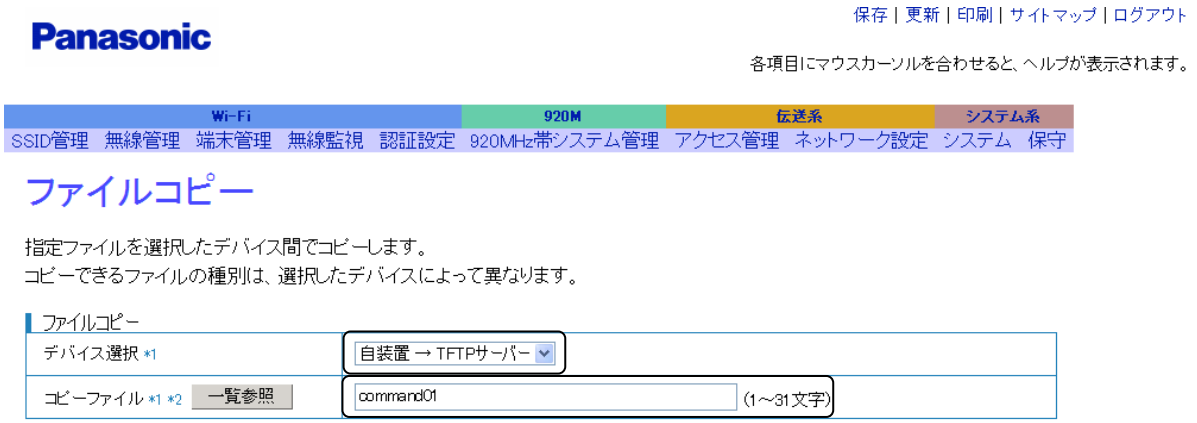


図7.3-17　ファイルコピー

以上の操作により、TFTP サーバに「コマンドログ」がコピー保存されます。

◆FTP によるログファイルコピー

FTP コマンドを使用してログファイルをコピーする場合、「6.1.1　設定データのバックアップ」を参照し FTP でログインします。ログイン後、「コマンド：“get command01”」を実行します。

7.3.4　ログの初期化

ログの初期化には、すべてのログを一括で初期化する方法と、各ログを個別に初期化する方法があります。
それぞれの手順を以下に示します。

操作手順

◆全ログクリアー

手順1　〔保守〕　→　〔初期化〕　→　〔ログ初期化〕を選択します。

図7.3-18　メニュー（ログ初期化）

手順2　全ログクリアーの〔全ログ〕のチェックボックスをクリックします。

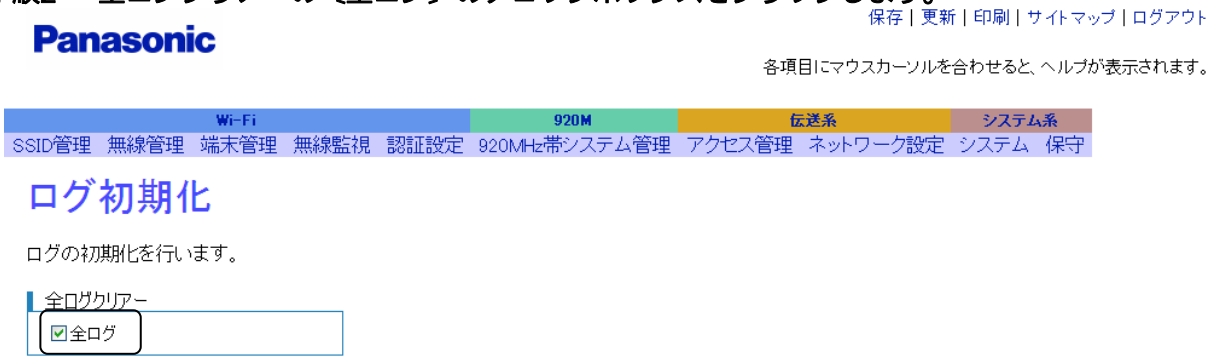


図7.3-19　ログ初期化（全ログクリアー）

手順3　画面最下部の〔実行〕をクリックします。

以上の操作により、すべてのログが削除されます。

◆各ログクリアー

例として、コマンドログの削除方法を紹介します。

手順1　〔保守〕　→　〔初期化〕　→　〔ログ初期化〕を選択します。

手順2　各ログクリアーの〔コマンドログ〕のチェックボックスをクリックします。

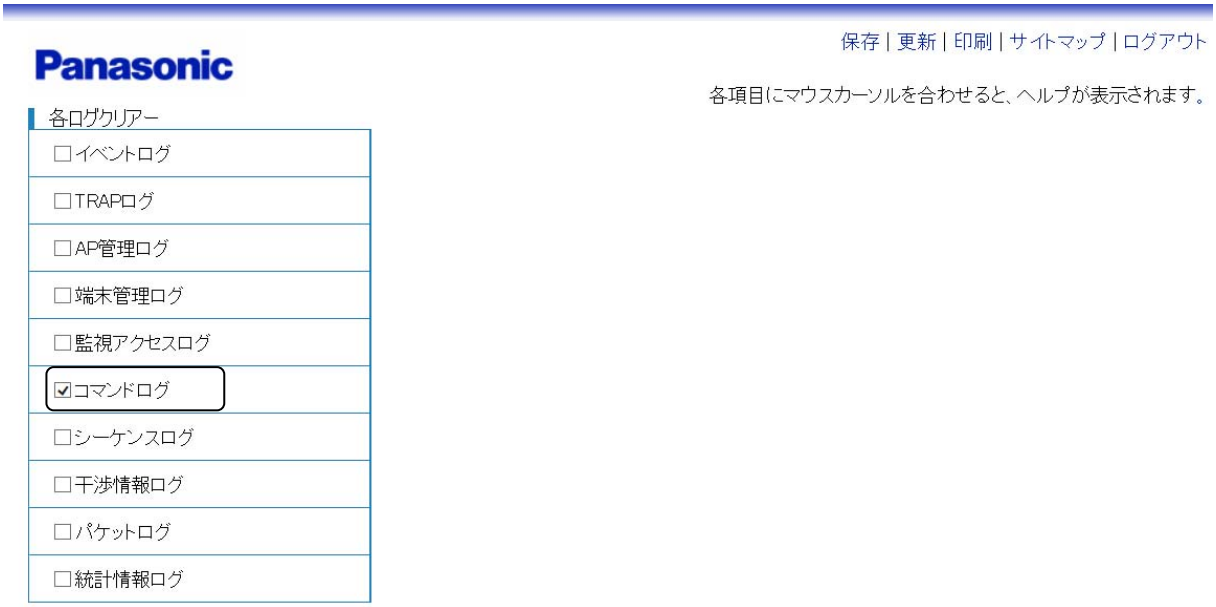


図7.3-20　ログ初期化（コマンドログクリアー）

手順3　画面最下部の〔実行〕をクリックします。

以上の操作により、コマンドログが削除されます。

7.3.5　干渉情報ログ・パケットログ・統計情報ログの読出し

コンセントレータでは、干渉情報ログ・パケットログ・統計情報ログの記録／読出しを行うことができます。読出し時は、ログ記録時の時刻を算出するために、ログデータの前にログ読出し時の現在時刻とログ読出し時の情報蓄積時間（sysUpTime）も読み出します。
各ログの記録方法は、「6.3.2　記録と表示」の　◆ログ機能の有効化、◆ログのファイル名設定、◆ログの記録方法の設定を参照してください。
ログが上限まで取得できていない場合は、蓄積分のみ取得可能です。

操作手順

手順1　〔システム系〕　→　〔保守〕　→　〔ファイルコピー〕を選択する。

図7.3-21　メニュー（ファイルコピー）

手順2　パケットログを TFTP サーバにコピーします。

以下の操作を行います。

- デバイス選択の〔自装置 → TFTP サーバ〕を選択
- コピーファイル名に ◆ログのファイル名設定で設定したファイル名を入力
  ここでは、「packetlog」を入力します。選択、および入力後、〔コピー〕をクリックします。

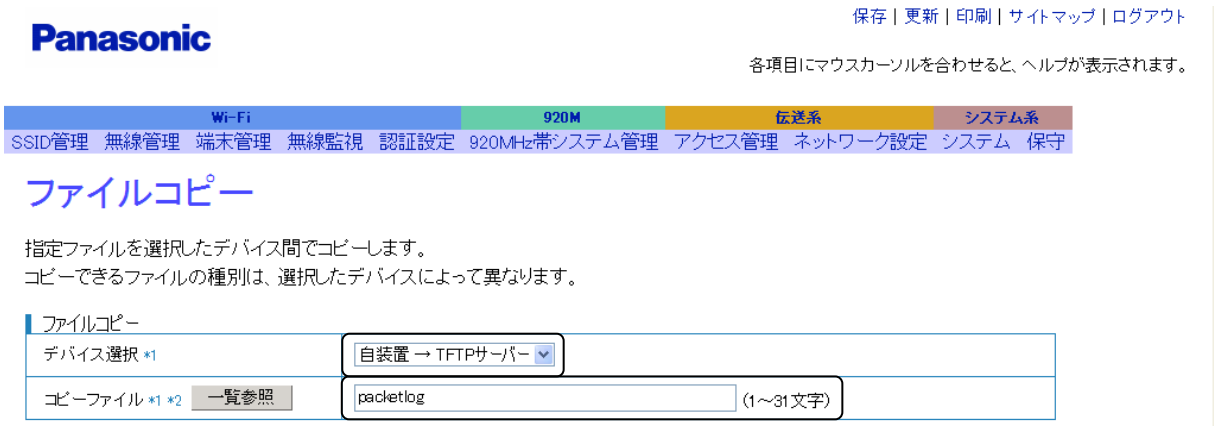


図7.3-22　ファイルコピー（パケットログ）

以上の操作により、TFTP サーバにパケットログがコピーされます。

7.4　遠隔無線通信状態の確認

コンセントレータでは、無線フレームが実際に送信されているかどうかを確認する無線送信検出機能を持ちます。
本機能は、無線フレームの送信状態を確認したい無線インターフェースを指定し、その無線インターフェースで送信した無線フレームを反対側の無線インターフェースで受信することにより、無線フレームの送信ができていることを確認する機能です。そのため、両無線インターフェースが有効の場合のみ検出処理を行います。どちらかの無線インターフェースが無効な場合は検出失敗となります。
なお、本機能では、ビーコンフレームを検出対象として使用します。

受信側の無線インターフェースで送信側のビーコンを受信した場合は、検出処理を終了します。
検出できない場合は、3 秒間検出処理を継続し、検出時間が満了した場合は、検出失敗（タイムアウト）として、検出処理を終了します。
※両無線インターフェース有効時に検出側の無線インターフェースのビーコン送信が無効に設定されている場合は、検出失敗（タイムアウト）となります。

重要	■ 通信状態検出処理中は、受信側の無線インターフェースを検出用に使用するため、受信側のビーコンフレームの送信は行いません。そのため、受信側の無線インターフェースでは、接続中の端末が切断される可能性があります。コンセントレータからの端末切断処理は行いません。

操作手順

手順1　〔Wi-Fi〕 → 〔無線管理〕 → 〔無線制御〕を選択します。

図7.4-1　メニュー（無線制御）

手順2　〔無線送信検出〕をクリックします。

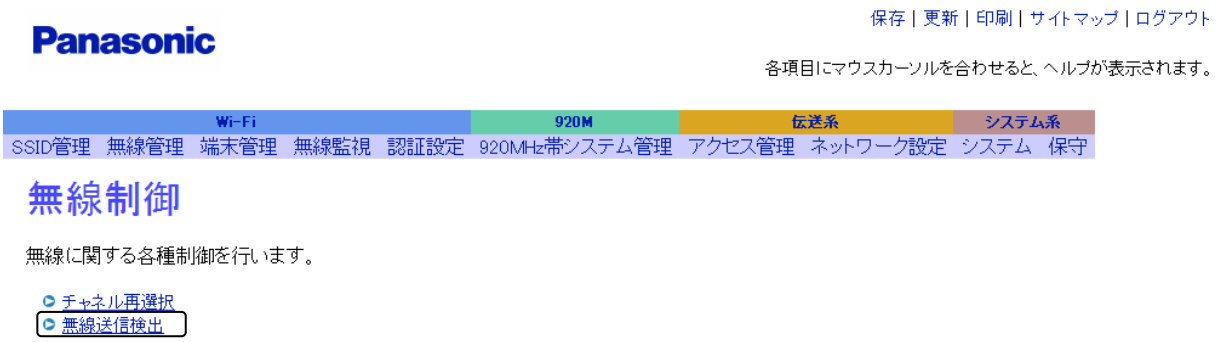


図7.4-2　無線制御

手順3　無線送信検出を実行します。

ここで選択した無線インターフェースを検出対象とします。

例として、〔IF1〕を選択します。

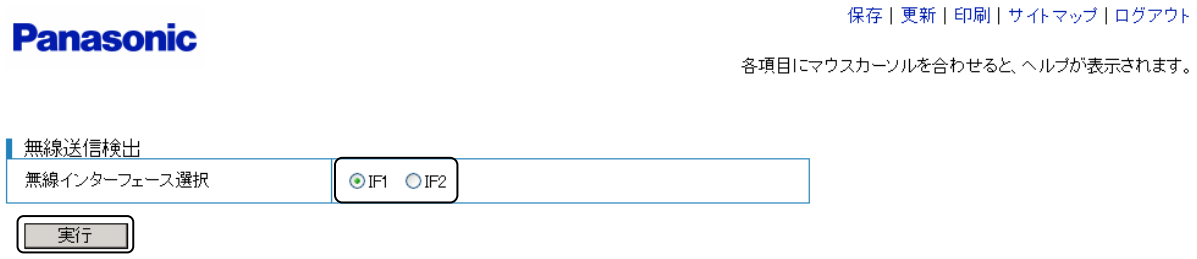


図7.4-3　無線制御送信検出

手順 3 実行後、下図の検出結果のダイアログボックスが表示されます。

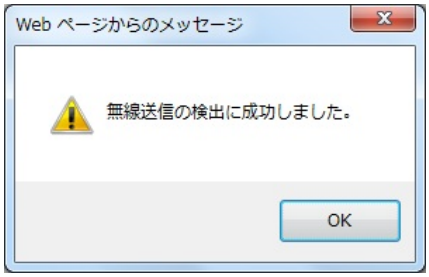


図7.4-4　検出成功時

7.5　時刻設定

Web コンソールからコンセントレータの時刻を設定できます。時刻設定方法として、手動による時刻設定とNTP クライアント機能を使用した時刻設定の 2 種類をサポートしています。

<NTP について>

ネットワーク機器の内部時計を、ネットワークを介して正しく調整するプロトコルです。階層構造を持ち、最上位のサーバがGPSなどを利用して正しい時刻を得て、下位のホストはそれを参照することで時刻を合わせます。

はじめに、手動による時刻設定の方法を示します。

操作手順

手順1　〔システム系〕　→　〔システム〕　→　〔運用設定〕　→　〔装置設定〕を選択します。

図7.5-1　メニュー（装置設定）

手順2　〔装置時刻〕をクリックします。

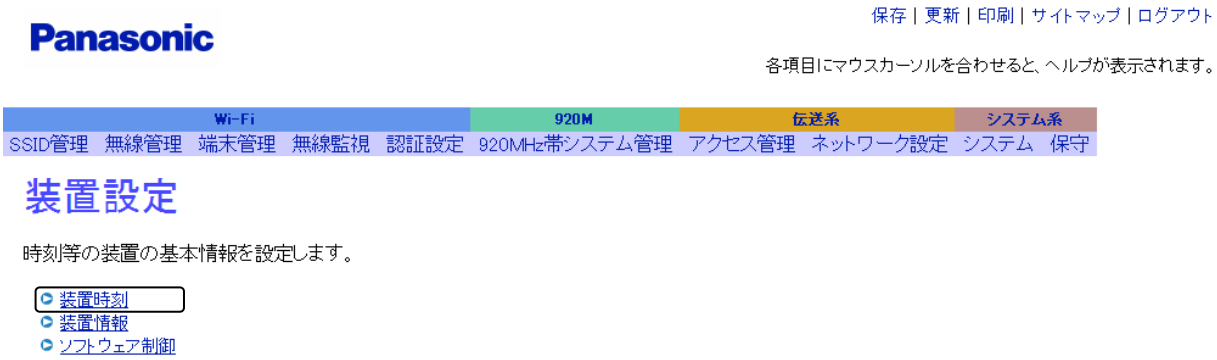


図7.5-2　装置設定

手順3　装置時刻を入力します。

例として、「2012/12/15 09:30:00」を入力します。

入力後、画面下部の〔設定〕をクリックしてコンセントレータに反映させます。

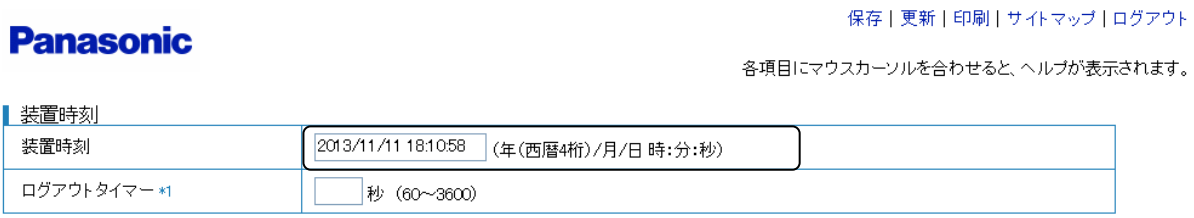


図7.5-3　装置時刻

以上の操作により、手動による時刻設定が行えます。

重要	■ 装置のリセットやコマンド入力による設定初期化および WEB での設定初期化（6.6　装置の初期化参照）を実行しても時刻の設定は初期化されることはありませんが、電源 OFF/ON で時刻が最大で 1 日巻き戻ります。また INIT スイッチによる初期化（6.6　装置の初期化参照）では時刻が「2000/1/1 00:00:00」に初期化されます。NTP クライアント機能を使用した時刻設定を行った場合は自動で時刻が補正されますが、設定を行っていない場合、電源 OFF/ON および INIT スイッチによる初期化の際には、必ず時刻設定を行ってください。 ■ ログ機能や IPsec 機能は装置時刻を参照していますので、これらの機能を正常に動作させるために、必ず時刻の設定を行ってください。

続いて、NTP クライアント機能を使用した時刻設定を以下に示します。

操作手順

手順1　〔システム系〕 →〔システム〕 →　〔監視設定〕 →　〔NTP 設定〕を選択します。

図7.5-4　メニュー（監視設定）

手順2　〔NTP 設定〕をクリックします。

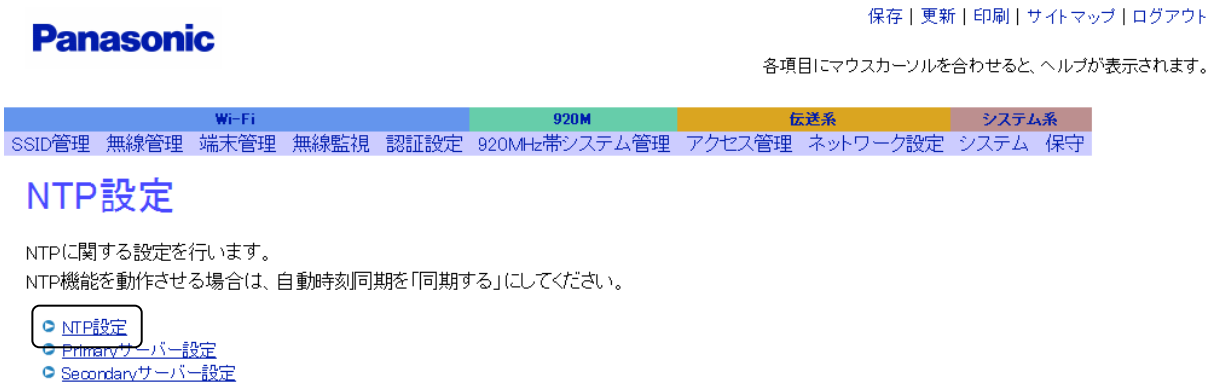


図7.5-5　NTP 設定

手順3　〔NTP 設定〕画面にて、〔同期する〕を選択します。

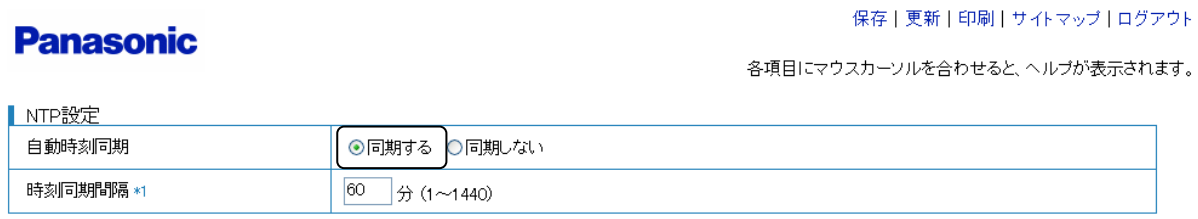


図7.5-6　NTP 設定

手順4　〔Primary サーバ設定〕画面にて、NTP サーバ（Primary）を設定します。

例として、下記内容での設定を示します。

- IP インターフェース番号：〔1〕を選択
- サーバ指定方法：〔IP アドレス〕を選択
- IP アドレス／ドメイン名：「192.168.0.76」を入力

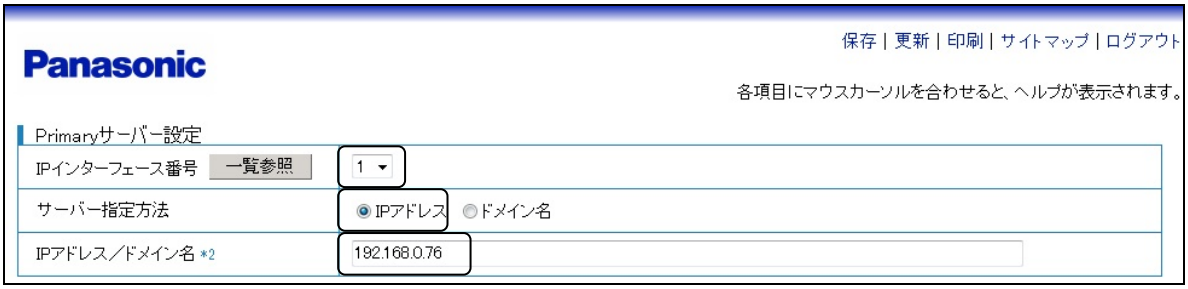


図7.5-7　Primary サーバ設定

手順5　〔Secondary サーバ設定〕画面にて、NTP サーバ（Secondary）を設定します。

例として、下記内容での設定を示します。

- IP インターフェース番号：〔1〕を選択
- サーバ指定方法：〔IP アドレス〕を選択
- IP アドレス／ドメイン名：「192.168.0.79」を入力

入力後、画面下部の〔設定〕をクリックしてコンセントレータに反映させます。

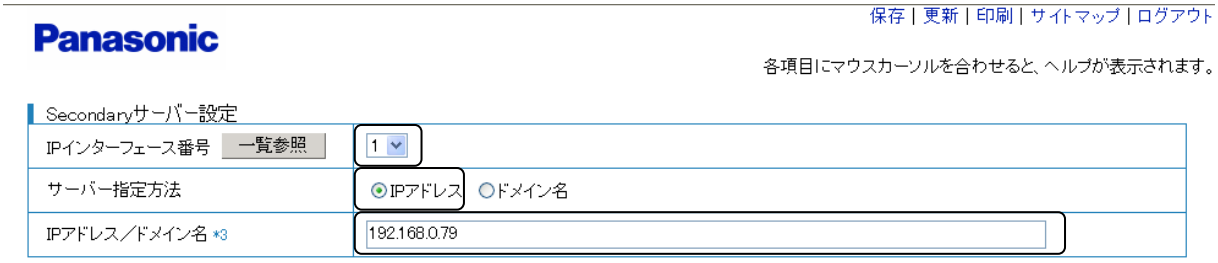


図7.5-8　Secondary サーバ設定

以上の操作により、NTP クライアント機能を使用した時刻設定が行われます。

手順 3、4 の「サーバ指定方法」で〔ドメイン名〕を選択する場合は、あらかじめ DNS サーバの設定が必要です。

7.6　装置の初期化

コンセントレータが持つ各種情報の初期化を行います。初期化方法は 3 種類あり、初期化される情報が異なります。

表6.6-1　初期化の種別一覧

初期化方法	初期化される情報
初期化スイッチ	すべての装置情報（設定データ、ログデータ、時刻情報、IKE 証明書データ）を工場出荷時の値にします。
コマンド入力	初期化を行いたい設定データ、またはログデータを指定することで、指定した情報のみを工場出荷時の値にします。
WEB	管理用インターフェースに関する設定以外、すべて初期化します。

※ 初期化を行った場合、元の状態に戻せなくなりますので、バックアップデータを取得する等、十分注意して行ってください。

操作手順

◆リセットスイッチでの設定初期化

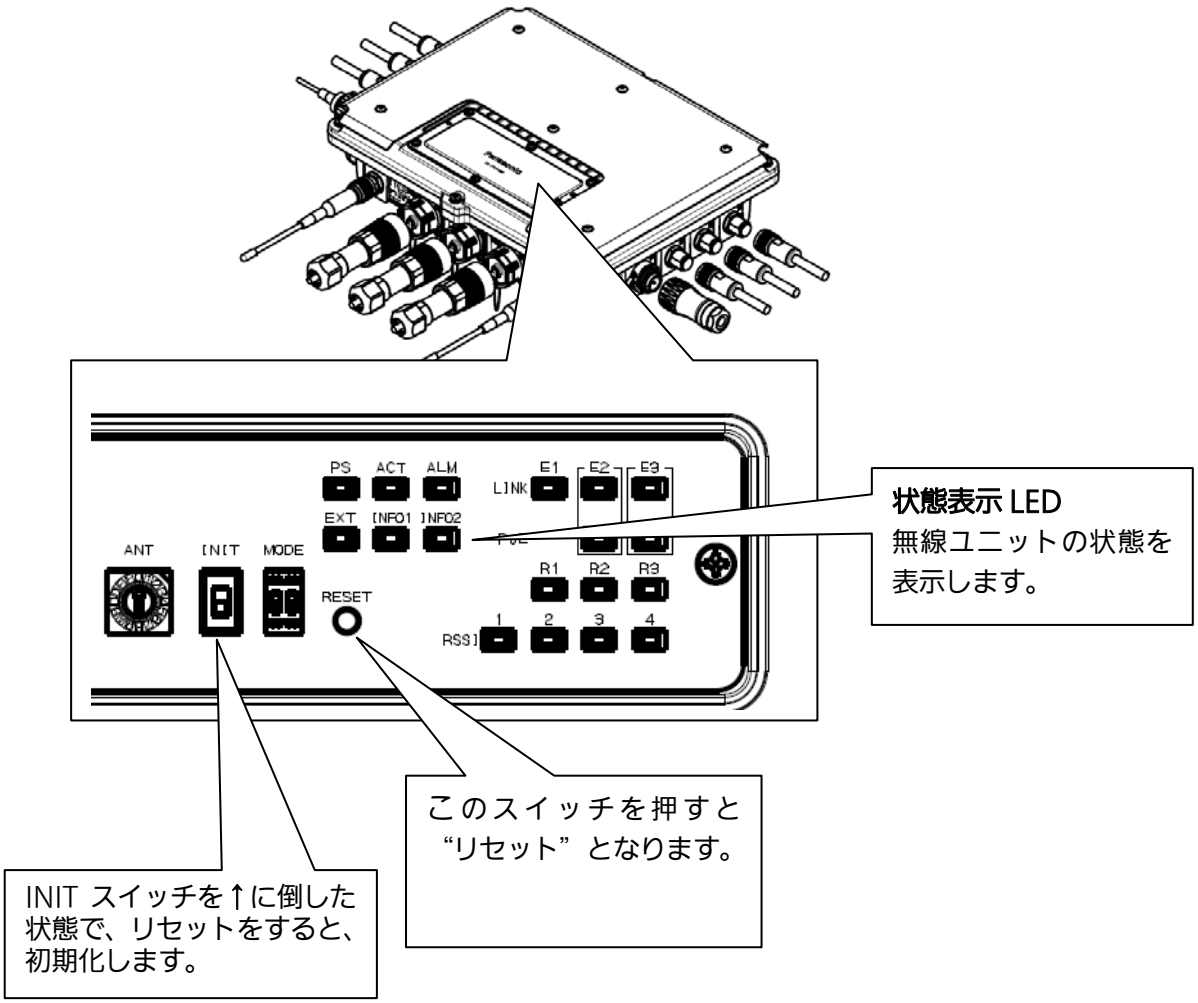
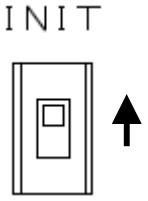


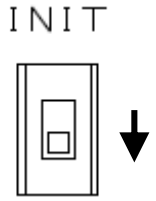
図7.6-1　マルチアクセス コンセントレータ配置説明

手順1　INIT スイッチを竹串など先端の細い棒で上側へ倒します。

※筐体の金属部に触る等で静電気を除去してから作業してください。



手順2　RESET スイッチを竹串など先端の細いもので押下してください。
手順3　ACT LED と ALM LED が点滅するのを待ちます。
手順4　ACT LED が点滅から点灯になりましたら、INIT スイッチを下側に戻し、
再度 RESET スイッチを押下してください。



以上で、INIT スイッチの操作による初期化が完了です。

＜初期化後の各インターフェースの初期値＞

インターフェース	初期設定	備考
WiFi インターフェース# 1 （R11,R12,R13）	無効	インターフェース有効設定後の初期値 2.4 GHz, 1ch, HT20 ANPDU+AMSDU
WiFi インターフェース# 2 （R21,R22,R23）	無効	インターフェース有効設定後の初期値 5.6 GHz, 100ch, HT40 ANPDU+AMSDU
920 MHz インターフェース （R31,R32）	無効	―
イーサネット （E1,E2,E3）	DHCP	AutoIP 機能により、起動後 20-30 秒後に”192.168.0.3”でアクセス可能になります。

◆コマンド入力による設定初期化

コンソールの接続が完了している前提で説明します。（コンソール接続方法は、2.4 CLI コンソールでのログイン・ログアウトを参照）

手順1　設定の初期化コマンドを入力して、実行します。

```
# initial config all
  ↑　初期化コマンドを入力します。
```

手順2　確認メッセージ表示後、“y”を入力して、実行します。

```
# initial config all
 “initialize” and “reset” y or n >>
  ↑　” y”　は「リセットし、初期化させる」、” n ”　は「リセットせず、初期化させない」
    となります。
```

上記「手順 2」実施後、コンセントレータが再起動し、設定データの初期化が完了します。

◆WEB での設定初期化

手順1　〔システム系〕　→　〔保守〕　→　〔初期化〕　→　〔設定初期化〕を選択します。

図7.6-2　メニュー（設定初期化）

手順2　〔クリアー〕をクリックします。

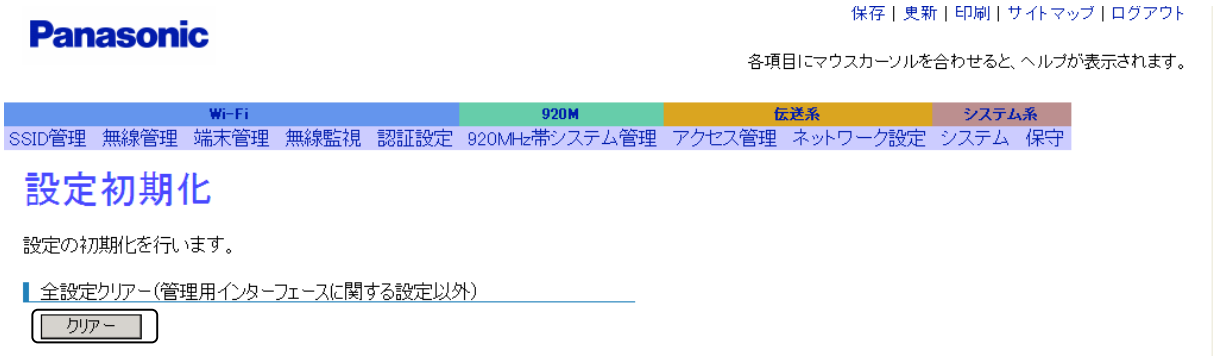


図7.6-3　設定初期化

手順3　確認メッセージの〔OK〕をクリックします。

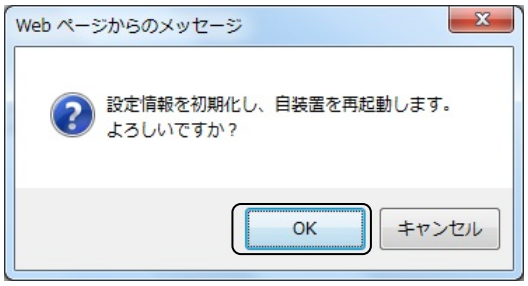


図7.6-4　初期化確認メッセージ

上記「手順 3」実施後、コンセントレータが再起動し、設定データの初期化が完了します。

保証とアフターサービス(よくお読みください)

使いかた・お手入れ・修理などは

■まず、お買い求め先へご連絡ください。

▼お買い上げの際に記入されると便利です

販売店名	
電話	（　　）　　－
お買い上げ日	年　　月　　日

修理を依頼されるときは

取扱説明書(工事編)「障害発生時の対処方法」でご確認の後、
直らないときは、電源（ブレーカ）を落として、お買い上げ日と下記の内容をご連絡ください。

● 製品名	マルチアクセス コンセントレータ / 920MHz 帯 通信ユニット
● 品番	EA-7TW11BS0 / EA-6HW11MS1
● 故障の状況	できるだけ具体的に

●保証期間中にマルチアクセス コンセントレータ、もしくは、920MHz 帯 通信ユニットが通常の使用状態で不良になった場合、修理は無償で実施します。

保障期間：お買い上げ日から本体 1 年間

●保証期間終了後は、診断をして修理できる場合はご要望により修理させていただきます。

※修理料金は次の内容で構成されています。

技術料　**診断・修理・調整・点検などの費用**

部品代　**部品および補助材料代**

出張料　**技術者を派遣する費用**

※補修用性能部品の保有期間 7 年

当社は、各装置の補修用性能部品（製品の機能を維持するための部品）を、
製造打ち切り後 7 年保有しています。

■その他ご不明な点は下記へご連絡ください。

パナソニック　システムお客様ご相談センター

電話　フリーダイヤル　0120-878-410（パナハ　ヨイワ）

携帯電話・PHS からもご利用いただけます。

受付時間：9 時 ～ 17 時 30 分（土・日・祝祭日は受付のみ）

ホームページからのお問い合わせは

https://sec.panasonic.biz/solution/info/

ご使用の回線（IP 電話やひかり電話など）によっては、回線の混雑時に数分で切れる場合があります。

【ご相談窓口におけるお客様の個人情報のお取り扱いについて】

パナソニック株式会社およびグループ関係会社は、お客様の個人情報をご相談対応や修理対応などに利用させていただき、ご相談内容は録音させていただきます。また、折り返し電話をさせていただくときのために発信番号を通知いただいております。なお、個人情報を適切に管理し、修理業務等を委託する場合や正当な理由がある場合を除き、第三者に開示・提供いたしません。

個人情報に関するお問い合わせは、ご相談いただきました窓口にご連絡ください。

パナソニック システムネットワークス株式会社

〒224-8539　神奈川県横浜市都筑区佐江戸町 600 番地

P1213-0

ⓒ Panasonic System Networks Co., Ltd. 2013